SMC6710L2
Intelligent 8+2G Switch
User's Manual

Version 1.0 (Oct. 2004)

We make no warranties with respect to this documentation and disclaim any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. We reserve the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

Trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies.

Contents

1. INTRODUCTION 1

1.1 PACKAGE CONTENTS 1

2. WHERE TO PLACE THE INTELLIGENT SWITCH 3

3. CONFIGURE NETWORK CONNECTION 3

3.1 CONNECTING DEVICES TO THE INTELLIGENT SWITCH 3
3.2 CONNECTING TO ANOTHER ETHERNET SWITCH/HUB 3
3.3 CONNECTING WITH TRUNK CONNECTION 4
3.4 APPLICATION 4

4. ADDING MODULE 6

4.1 ADDING MINIGBIC(SFP) MODULE 6

5. LEDS CONDITIONS DEFINITION 7

5.1 LEDS DEFINED 7

6. MANAGE / CONFIGURE THE SWITCH 9

6.1 INTRODUCTION THE MANAGEMENT FUNCTIONS 9
6.2 MANAGEMENT WITH CONSOLE CONNECTION 12
6.3 MANAGEMENT WITH HTTP CONNECTION 36
6.4 ABOUT TELNET INTERFACE 59
6.5 ABOUT SNMP INTERFACE 59

7. SOFTWARE UPDATE AND BACKUP 60

A. PRODUCT SPECIFICATIONS 61

B. COMPLIANCES 62

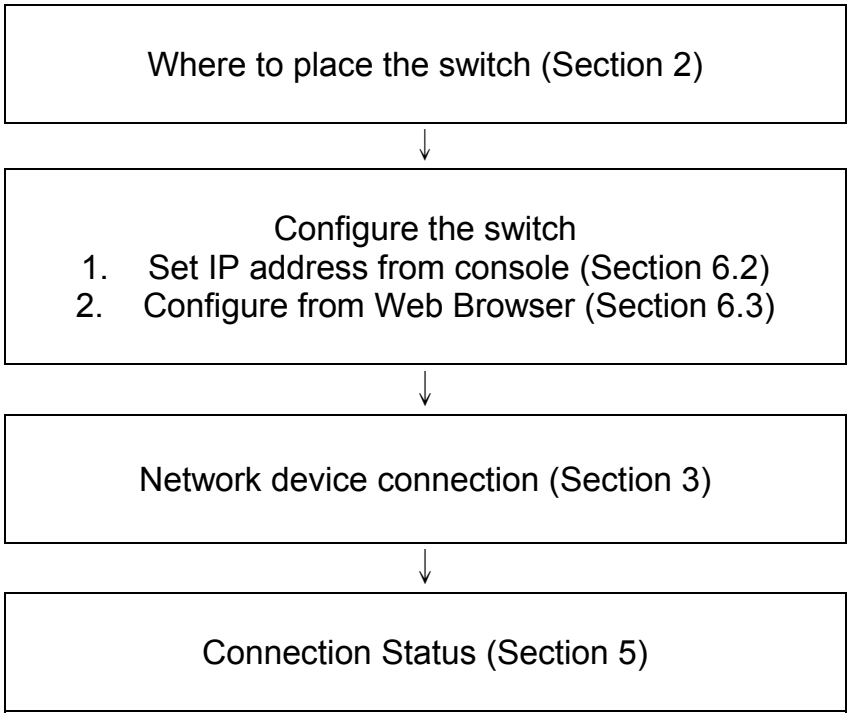
1. Introduction

This switch is a cost-effect high performance 8TX + 2Gigabit ports 10/100/1000 Mbps Ethernet/Fast Ethernet/Gigabit Ethernet management switch with Broadcom solution. There are two built-in gigabit ports for high-speed users and high-speed connections.
This switch supports remote management function by SNMP, Http and Telnet operations. It supports lots of functions for a L2 switch management, e.g. VLAN(port-based/802.1Q), System Configuration, Port Configuration, Port Mirroring, Port Statistics, QoS functions, IGMP snooping. Auto-MDIX function is also supported for every TX port of the switch for easy cable connection.

1.1 Package Contents

- One Intelligent Switch
- One AC power cord
- One console cable
- One set of 19inch rackmount kit
- Four rubber feet
- This user's manual

Installation Procedure


Where to place the switch (Section 2)
Configure the switch
1. Set IP address from console (Section 6.2)
2. Configure from Web Browser (Section 6.3)
Network device connection (Section 3)
Connection Status (Section 5)

2. Where To Place the Intelligent Switch

This Intelligent Switch can be placed on a flat surface (your desk, shelf or table). Place the Intelligent Switch at a location with these connection considerations in mind:

- The switch configuration does not break the rules as specified in Section 3.
- The switch is accessible and cables can be connected easily to it.
- The cables connected to the switch are away from sources of electrical interference such as radio, computer monitor, and light fixtures.
- There is sufficient space surrounding the switch to allow for proper ventilation (the switch may not function according to specifications beyond the temperature range of 0 to 50 degrees C).

3. Configure Network Connection

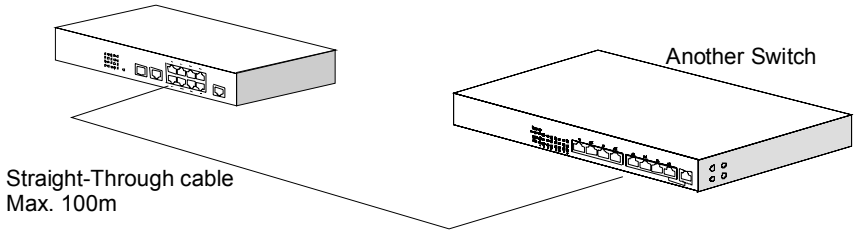
3.1 Connecting Devices to the Intelligent Switch

[Connection Guidelines:]

- For 10BaseT connection: Category 3 or 5 twisted-pair Ethernet cable
- For 100BaseTX connection: Category 5 twisted-pair Ethernet cable
- For 1000BaseT connection: Category 5e twisted-pair Ethernet cable
- For UTP cable connection, always limit the cable distance to 100 meters (328 ft) as defined by IEEE specification
- Because this switch supports **Auto MDI/MDI-X** detection on each UTP port, you can use normal straight through cable for both workstation connection and hub/switch cascading.

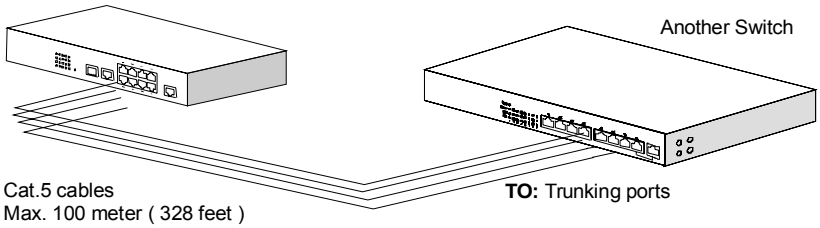
3.2 Connecting to Another Ethernet Switch/Hub

This Intelligent Switch can be connected to existing 10Mbps/100Mbps/1000Mbps hubs/switches. Because all UTP ports on the Intelligent Switch support Auto MDI/MDI-X function, you can connect from any UTP port of the Intelligent Switch to the MDI or MDI-X port of another hub/switch with Straight Through or Crossover cables.



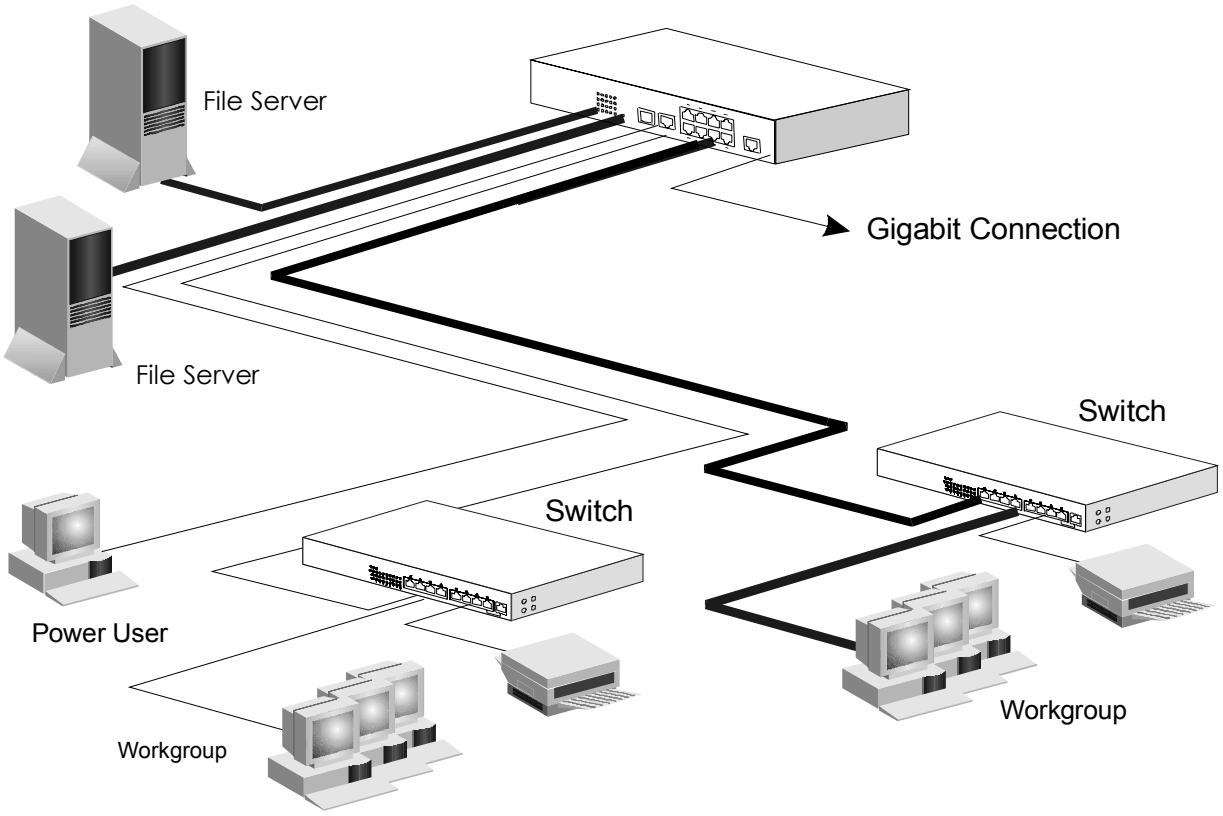
3.3 Connecting with Trunk connection

This switch supports trunk function for high-speed connection between switches to remove the bottleneck problem of switch-to-switch connection. The bandwidth of the trunk connection is the total bandwidth of the cables in the trunk. For example, Port 1,2,3,4 are used for trunk connection and the trunk bandwidth is 200Mbps x 4 = 800Mbps.
Because all UTP ports of the Intelligent Switch support Auto MDI/MDI-X function, you can connect from the trunking ports of the Intelligent Switch to the trunking ports of another hub/switch with Straight Through or Crossover cables.
Notes: Please enable and configure the trunk function first before connecting cables to prevent packet looping between switches.



3.4 Application

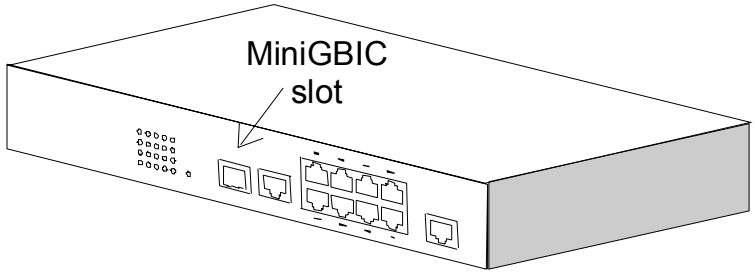
A switch can be used to improve overall network performance. Switches make intelligent decisions about where to send network traffic based on the destination address of the packet. As a result, the switch can significantly reduce unnecessary traffic.
The example below demonstrates the switch ability to segment the network. The number of nodes on each segment is reduced thereby minimizing network contention (collisions) and boosting the available bandwidth per port.
With management function of the switch, network administrator is easy to monitor network status and configure for different applications.


File Server
Gigabit Connection
File Server
Switch
Switch
Power User
Workgroup
Workgroup

4. Adding Module

4.1 Adding MiniGBIC(SFP) Module

A MiniGBIC module slot for gigabit connection extension is supported at front panel. You can add a MiniGBIC module to the switch and this switch gets another gigabit port.



Please follow the steps to add the module to the switch.

1. Slide in the module into the module slot.
2. Connect network cable to the port of the module.

5. LEDs Conditions Definition

5.1 LEDs Defined

The LEDs provide useful information about the switch and the status of all individual ports.

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
LINK / ACT	ON	Port has established a valid link.
	Flashing	Packets being received or sent.
FDX	ON	The connection is Full Duplex.
	OFF	The connection is Half Duplex.

6. Manage / Configure the switch

6.1 Introduction the management functions

This switch is a L2 management switch. It supports in-band management function from SNMP, Http and Telnet interface. It also supports out-band management function from RS232 console interface. Besides, it supports network configuration functions, like VLAN, Trunking, Port Mirror, QoS, spanning tree and software backup/update. Users can configuration these functions for different network applications. The following is a brief introduction about these functions before the detail operation sections.

1. VLAN (Virtual LAN)
   VLAN can divide the switch to several broadcast domains to prevent network traffic between different user groups. This switch supports Port-based and 802.1Q tag-based VLAN. Users in the same VLAN can transfer data to each other. The network traffic will be blocked if they are in different VLANs.

2. Trunk
   If two switches are cascaded together, the bottleneck will happen at the cascading connection. If more cables could be used for the cascading connection, it will reduce the bottleneck problem. In normal case, switches will become unstable because of traffic looping when more than one cable is connected between them. If the switches support trunk function, they can treat these cables as one connection between them. The traffic looping will not happen between these cables and the switches will work stable with bigger bandwidth between them.
   This switch supports trunk function and users can configure it with the following steps.
   a. Enable trunk function.
   b. Select the port partition for trunk.
   c. Assign ports to a trunk. For example, assign Port 1,2,3 for Trunk 1.

   Notes: About redundant application
   The trunk connection supports redundant function. If any trunk cable is broken, the traffic going through that cable will be transferred to another trunk cable automatically. For example, if user port Port 6 is assigned to Port 1 in a Trunk and Port 1 connection breaks, Port 2 will take over the traffic for Port 6 automatically. (It could be used for redundant application.)

3. Spanning Tree Protocol
   Spanning tree is a protocol to prevent network loop in network topology. If network loop happens, it will cause switches in the network unstable because more and more traffic will loop in the network. If network loop happens, spanning tree protocol will block one connection in the loop automatically. But

it will also cause a 30 seconds delay if any network connection is changed because of the network topology detection operation of the protocol.
Because there could be more than one switch in the network, users can configure this function for their network spanning tree application.

4. Port Mirror
   This switch operates in store-and-forward algorithm so it is not possible to monitor network traffic from another connection port. But the port mirror function could copy packets from some monitored port to another port for network monitor. This switch also provides DA/SA filtering function for monitoring the traffic to/from some user

5. QoS
   For Quality of Service request in a network, packets could be classified to different forwarding priorities. For real-time network traffic (like video, audio), it needs higher priority than normal network traffic. With the definition of packet priority, it could have 8 priority levels (from 0 to 7). This switch supports two priority level queues on each port. It could be configured for port-based or 802.1P tagged based. User can define the threshold (0 – 7) between high and low priority queues. And user can also define the weight of traffic between the high and low priority queues.

6. Static Mac ID in ARL table
   The switch can learn the Mac address from user's packets and keep these Mac address in the ARL table for store-and-forward table lookup operation. But these Mac addresses will be deleted from ARL table after some time when users do not send any packets to the switch. This operation is called aging and the time is called aging time. It is 5 minutes normally (it could be changed by users.) If users want to keep a Mac address always in ARL table for some port, they can assign the Mac address to ARL table. These Mac ID are called Static Mac address. This switch supports static Mac address assignment. *The static Mac address assignment will also limit the Mac address could be used on the assigned port only.* For example, assigning "00-c0-f6-11-22-33" to Port 5 will always keep this Mac ID alive on Port 5 but also limit this Mac address could work on Port 5 only.

   Note: About Static Mac Address Filter-in (port binding) function
   There is a "Mac Security Configuration" function for port security. Only these static Mac addresses can access network through the assigned port. The other Mac addresses will be forbidden for network access through that port. This function can be used for port binding security application. Please refer to Section 6.2 / 6.3 for the details of the Mac address filter-in operation of the switch.

7. IEEE 802.1x Port Security Function
   If the 802.1x function is enabled, the switch will act as an authenticator for users accessing network through the switch. It will need a RADIUS server for the authentication function. Users will be asked for username and password before network access. If the RADIUS server authenticates it, the switch will

enable the port for network access. This function is very useful for network security application to prevent illegal users access network through the switch. This switch supports MD5, TLS and PEAP authentication types.

8. IGMP Snooping Function
   This switch can forward IP multicast packets according to the IP multicast group definition. The IP multicast group information is learned from the packets of IGMP active router with the snooping operation. You have to define the routing port (the port that connecting to the IGMP active device) first for this function.

9. Software Backup/Update
   This switch supports backup and update functions for its internal software and its network configuration. It could be done in three ways.

   a. From console when booting : doing by Xmodem protocol and by terminal program for boot code and run-time code updating.

   b. From console/Telnet when running : doing by TFTP protocol and it will need a TFTP server in network for run-time code and configuration backup/update.

   c. From web browser : doing by http protocol and by web browser for run-time code and configuration backup/update.

6.2 Management with Console Connection

Please follow the steps to complete the console hardware connection first.

1. Connect from the console port of the switch to COM port of PC with the console cable.
2. Start the terminal program of Windows. Create a new connection and select COM port of PC used for the console. Set the configuration of the terminal as **[38400,8,N,1]**. (You can find the terminal program in [Start] -> [Programs] -> [Accessory Programs] -> [Communication] -> [Terminal]. If you cannot find it, please install it from your Windows Installation Disk. Please refer to your Windows user manual for the installation.)
3. Power on the switch.

If everything is correct, the booting screen will appear in the terminal program when the switch is powered on. It will stop at the following screen after some initializing messages.

```
---------------------------------------------------------------------------------------------
Booting Program Version 1.01.00, built at 16:06:25, Feb 19 2003

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05a00000, 32 blocks of 0x00010000 bytes each.
==> enter ^C to abort booting within 3 seconds .....


Start to run system initialization task.
[System Configuration]
Company Name    :
Model Name      : Intelligent Switch
MAC  Address    : 00:C0:F6:01:01:01


Firmware version: 2.20.03 (built at Oct  1 2004 12:51:44)
Press <ENTER> key to start.
UCD-SNMP version 4.1.2
---------------------------------------------------------------------------------------------
```

Press Enter key, user name and password will be requested. The default user name and password is "**admin**" / "**123456**".
After login the switch, a prompt will be shown. Because this switch supports command-line for console interface, you can press "**?**" or "**help**" to check the command list first.

Note: Management with **Telnet** connection has the same interface as console connection.

With **help** command, you can find the command list as follow.

```
---------------------------------------------------------------------------------------------------
>help
[Command List]
?..... Help commands
backup..... backup run-time firmware or configuration file
del..... Del commands
find..... Find commands
exit..... Logout
help..... Help commands
logout..... Logout
ping..... Ping a specified host with IP address
reset..... Reset system or reset factory default setting
set..... Set commands
show..... Show commands
upgrade..... Upgrade run-time firmware or configuration file
>
---------------------------------------------------------------------------------------------------
```

Here is the detail about these commands.

1. **Backup** command
   This switch supports TFTP protocol for firmware and configuration update and backup. You should select backup *firmware* or *configuration* first. And provide the IP address of the TFTP server and the backup file name for the backup operation.

   Enter “backup” at the prompt, the command syntax will be shown.
   ```
   >backup
   Syntax: backup [firmware | config] ip filename
   ```

   For example, “back config 192.168.1.80 abcd” will backup the configuration to TFTP server 192.168.1.80 and its file name is “abcd”.

2. **Del** command
   The “del” command can delete staic entries in ARL table, disable Mirror function, remove ports in a trunk group, remove forwarding ports for trunk port.

   Enter “del” at the prompt, the command syntax will be shown.
   ```
   >del
   [Command List]
   ?..... Help commands
   help..... Help commands
   arl..... Delete a specified MAC address from ARL table
   vlan..... Destroy a specified VLAN ID
   trunk..... Destroy a specified trunk group of port-based trunk
   mactrunk..... Destroy a specified trunk group of MAC-based trunk
   trunkforward... Destroy a specified trunk forwarding port
   ```

   - *Delete static entries in ARL table . . .*

>del arl
Del ARL [xx-xx-xx-xx-xx-xx]

xx-xx-xx-xx-xx-xx is a assigned static Mac ID in ARL table of the switch. You can remove it from the table with the command. For example, “del arl 00-11-22-33-44-55” will delete the static Mac ID “00-11-22-33-44-55” from ARL table.

- *Remove a VLAN Group . . .*

>del vlan
Syntax: del vlan [vlan#]

[vlan#] is the VLAN ID.

- *Remove All Ports in a Port-based Trunk Group . . .*

>del trunk
Syntax: Del TRUNK [trunk#]

[trunk#] is the trunk group number and all the trunk ports in this trunk will be removed by this command. This command is for Port-based trunk. The traffic assignment in Port-based trunk is based on physical port of the traffic and is assigned manually. For example,”del trunk 3” will remove all trunk ports from Trunk 3 and Trunk 3 becomes a null trunk.

- *Remove All Ports in a Mac-based Trunk Group . . .*

>del mactrunk
Syntax: del mactrunk [trunk#]

[trunk#] is the trunk group number and all the trunk ports in this trunk will be removed by this command. The traffic assignment in Mac-based trunk is based on the Mac address of the traffic. For example, ”del trunk 3” will remove all trunk ports from Trunk 3 and Trunk 3 becomes a null trunk.

- *Remove All Forwarding Ports from a Port-based Trunk Port . . .*

>del trunkforward
Syntax: del trunkforward [port#]

This command will delete the forwarding port list for a Port-based trunk port. For example, Port 5 is a trunk port in Trunk 3 and Port 1,2,3 are assigned to go through Port 5 in this trunk. “del trunkforward 5” will delete the forwarding port list Port 1,2,3 for Port 5 and no any traffic will go through Port 5. If you want to assign traffic of Port 1,2,3 to go through another trunk port, please use “set trunkforward” command to add them to another trunk port. Otherwise, no trunk port will work for the traffic of Port 1,2,3 in the trunk connection.

3. **Find** command
   The “find” command can find a static Mac address in the ARL table.

   Enter “find” at the prompt, the command syntax will be shown.
   ```
   >find
   [Command List]
   ?..... Help commands
   help..... Help commands
   arl..... Search a specified MAC address in ARL table
   ```

   The syntax is as follow.
   ```
   >find arl
   Find ARL [xx-xx-xx-xx-xx-xx]
   ```

   If the Mac address is a static address in ARL table, it will be shown as follow.
   ```
   >find arl 00-c0-f6-11-22-33
   This MAC [00-c0-f6-11-22-33] is in port [2]!
   ```

   If the Mac address is not a static address in ARL table, it will be shown as follow.
   ```
   >find arl 00-c0-f6-77-88-99
   Failed!
   ```

4. **Exit** command
   This is a logout command – the same as Logout command.

5. **Help** command
   This is a help command (the same as “?” command) and the switch will prompt command list for this command.

6. **Logout** command
   This is a logout command – the same as Exit command.

7. **Ping** command
   User can use this command to ping another network device to verify the network connection and activity. (It is similar to the ping command in MS-DOS.)

   Enter “ping” at the prompt, the command syntax will be shown.
   ```
   >ping
   Syntax: ping [-n count] [-l length] [-t] [-w timeout] ip
   -n count  : Number of echo requests to send.
   -l length : Send buffer size, and length is between 64~8148
   -t        : Ping the specified host until stopped by <ESC> key.
   -w        : Timeout in milliseconds to wait for each reply.
   ip        : IP address (xxx.xxx.xxx.xxx)
   ```

   For example, ping 192.168.1.80. “Ctrl-C” can be used to break continuous ping operation.

8. **Reset** command
   The command can be used to reset switch or restore factory default setting.

Enter “reset” at the prompt, the command syntax will be shown.

```
>reset
Syntax: reset [configuration | system]
```

“reset configuration” will restore the configuration to the factory default setting.
“reset system” will reset the switch and the switch will reboot.

9. **Set** command

This command can be used to configure most functions of the switch. Lots of sub-commands are needed for this command.

Enter “set” at the prompt, the sub-command list will be shown.

```
>set
[Command List]
?..... Help commands
help..... Help commands
admin..... Set administrator name and password
arl..... Add a static MAC address in ARL table
eth0..... Set network eth0 configuration
idle..... Set idle time for CLI session.
igmp..... Set IGMP configuration
mirror..... Set mirror configuration
age..... Set switch age
automode..... Set Auto Negotiation or Auto Detect mode
port..... Set switch port configuration
qos..... Set QoS configuration
snmp..... Set snmp configuration
trunk..... Set a port to join/leave a specified port-based trunk group
mactrunk..... Set a port to join/leave a specified MAC-based trunk group
trunkforward... Set a port to join/leave a specified trunking port
vlan..... Set a port to join/leave a specified VLAN Group
1qvlan..... Set 802.1Q
dot1x..... Set 802.1x Configuration
security..... Set MAC Security Configuration
sta..... Set Spanning Tree  setting
http..... Set HTTP Protocol setting
```

9.1 **set ?** and **set help** command

These two commands will show the sub-command list for “set” command.

9.2 **set admin** command

This command can be used to modify the user name and password for administrator.

9.3 **set arl** command

This command is for adding static Mac ID to ARL table of the switch.

It syntax is . . .

```
>set arl
Set ARL [xx-xx-xx-xx-xx-xx] [port#,port#,...] [high/low]
```

For example, “set ARL 00-c0-f6-11-22-33 5 low” will add a static Mac ID “00-c0-f6-11-22-33” to ARL table for Port 5 with low priority and this Mac ID will never be aged out from Port 5.

Note: Because the static Mac address is fixed on the assigned port, the static Mac address can access network through the assigned port only. If Mac security function is enabled on the port, only the user with the static address can access network through the port.

9.4 **set eth0** command

This command is used to configure IP address of the switch.

Its syntax is . . .

```
>set eth0
[Syntax]set eth0 [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
ip..... Set IP Address
netmask..... Set netmask
gateway..... Set gateway IP address
```

For example, “set eth0 ip 192.168.1.250 netmask 255.255.255.0 gateway 192.168.1.154” will set these parameters as the IP address configuration of the switch. After the command, you can use “show net” to verify the setting.

Note: We suggest you to reset the switch after modifying IP configuration.

9.5 **set idle** command

This command is used to set idle time for console connection. If no any key operation in this idle time, the switch logout automatically for security.

Its syntax is . . .

```
>set idle
Syntax: Set idle [timeout value]
```

For example, “set idle 300” will change the idle time to 300 seconds. It is 10 minutes default. Its valid range is 30 ~ 3600 seconds.

9.6 **set igmp** command

This command is used to set the IGMP function of the switch.

Its syntax is . . .

```
>set igmp
[Command List]
enable..... Enable IGMP function
disable..... Disable IGMP function
routerport..... Set IGMP router port
```

For example, “set igmp routerport 2” will set the IGMP active connection is at Port 2 of the switch. You have to assign the port that connects IGMP active device first for IP multicast operation.

9.7 **set mirror** command

This command is used to configure mirror port function. The following is the sub-command for it.

```
>set mirror
[Command List]
ingress..... Set mirror ingress setting
egress..... Set mirror egress setting
port..... Set mirror capture port setting
enable..... Enable mirror function
disable..... Disable mirror function
```

9.7.1 **set mirror ingress** command

This command is used to configure the mirror operation for ingress traffic. Its syntax is . . .

```
>set mirror ingress
[Syntax]set mirror ingress [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
div..... Set mirror ingress/egress [div=%d]
mode..... Set mirror ingress/egress [mode=ALL/SA/DA]
mac..... Set mirror ingress/egress [mac=xx-xx-xx-xx-xx-xx]
monitor..... Set mirror ingress/egress [monitor=xx,xx,xx]
```

set mirror ingress div x : every x packets, capture one for mirror. For example, “set mirror ingress div 10” will capture one packet from every ten packets from ingress traffic.

set mirror ingress mode xx : mirror all packets or mirror packets with some DA or SA only. For example, “set mirror ingress mode all” will mirror all packets.

set mirror ingress mac xx-xx-xx-xx-xx-xx : if the mirror mode is for the packets with some DA/SA, users can assign the DA/SA here.

set mirror ingress monitor xx,xx,xx : set the monitored ports here. For example, “set mirror ingress monitor 1,2,5” will mirror the ingress traffic from Port 1,2,5. (Notes: If the monitored traffic exceeds the maximum bandwidth of capture port, flow control function will work on these monitored ports.)

9.7.2 **set mirror egress** command

This command is used to configure the mirror operation for egress traffic. Its syntax is similar to the mirror operation for ingress traffic. Please refer to “**set mirror ingress** command” section.

9.7.3 **set mirror port** command

This command is used to set the capture port for mirror operation. For example, “set mirror port 3” will capture the mirror traffic to Port 3.

9.7.4 **set mirror enable** command

This command is used to enable the mirror operation.

9.7.5 **set mirror disable** command

This command is used to disable the mirror operation.

9.8 **set age** command

This command is used changed the aging time of the switch.
Its syntax is . . .

```
>set age
Syntax: set age [time]
```

The aging time is 300 seconds default and its valid range is 0 ~ 65535.
If [time] is set to 0, the aging function will be disabled. (Notes: It is different from static Mac ID in ARL table. The connection port is fix for a static Mac ID, but the connection port could be changed for a Mac ID with no aging.)

9.9 **set automode** command

This command is used to set the auto mode function of connection ports. There are two modes for it – an(auto negotiation) and ad(auto detection).

an mode – if the *auto mode* of a port is disabled in port configuration, the switch will disable its auto-negotiation function and the Auto-MDIX function of the port is also disabled. That is the real force-mode setting of the port.

ad mode – if the *auto mode* of a port is disabled in port configuration, the switch will not disable its auto-negotiation function but just modify its auto-negotiation attribute for the speed/duplex mode setting. And the Auto-MDIX function of the port is still enabled.

If the connected device is *auto-negotiation enabled* and you want to set the speed of the connection (for example, 10M/Half), you can select ad mode. If the connected device is in forced mode (for example, 10M/Half) and it is *auto-negotiation disabled*, you can use an mode and set the port to the same configuration as the device in port configuration function.

You can select an mode or ad mode depending on your applications. In most of the connection cases, ad mode is suggested.

9.10 **set port** command

This command is used to change the connection configuration of ports.
Its syntax is . . .

```
>set port 1
[Syntax]set port [port#] [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
name..... Set port name [string]
admin..... Set port admin mode [enable|disable]
speed..... Set port speed [auto|10|100|1000]
duplex..... Set port duplex type [full|half]
flow..... Set port flow mode [enable|disable]
```

User can configure the following items for each port.
a. *Name of a port* with "**name**" sub-command.
b. *Enable/Disable a port* with "**admin**" sub-command.
c. *Operation speed of a port* with "**speed**" sub-command.
d. *Duplex mode of a port* with "**duplex**" sub-command.
e. *Flow control function of a port* with "**flow**" sub-command

For exampe, "set port 1 name YYY admin enable speed 10 duplex half" command will enable Port 1 and set it to 10Mbps/Half Duplex and name it as "YYY".

9.11 **set qos** command

This command is used to configure QoS function of the switch.

Its syntax is . . .

```
>set qos
[Syntax]set QoS [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
enable..... Set QoS enabled. Syntax: Set QoS enable
disable..... Set QoS disabled. Syntax: Set QoS disable
priority..... Set QoS priority of specified port.
   Syntax: Set QoS priority [port#] [high/low]
hq..... Set HQ setting. Syntax: Set QoS HQ=xxx (0~15)
lq..... Set LQ setting. Syntax: Set QoS LQ=xxx (0~15)
pt..... Set 802.1p setting. Syntax: Set QoS PT=xxx (0~7)
```

This switch supports two priority queues on each port – high priority queue and low priority queue. Both port-based priority and 802.1P tag priority are supported. This function can be used to configure high/low priority queues of the switch. Here are the details about these sub-commands.

9.11.1 **set qos enable** command

This command is used to enable QoS operation.

9.11.2 **set qos disable** command

This command is used to disable QoS operation.

9.11.3 **set qos priority** command

This command is used to configure port-based priority. All packets coming from high priority port will always be forwarded to high priority queue. For example, "set qos priority 3 high" command will set Port 3 as a high priority port.

9.11.4 **set qos hq** command

This command is used to set the weight of traffic rate for high priority queue. For example, "set qos hq=10" command will set the weight of traffic rate for high queue to 10.

9.11.5 **set qos lq** command

This command is used to set the weight of traffic rate for low priority queue. For example, “set qos lq=3” command will set the weight of traffic rate for low priority queue to 3.

9.11.6 **set qos pt** command

This command is used to set the threshold of high priority queue and low priority for 802.1P tagged packets. The priority value in 802.1P tagged packet could be 0 ~ 7. For example, with “set qos pt=4” command, the 802.1P tagged packets with priority values 4~7 will go to high priority queue and packets with priority values 0~3 will go to low priority queue.

9.12 **set snmp** command

This command is used to configure SNMP function of the switch.

Its syntax is . . .

```
>set snmp
[Syntax]set snmp [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
name..... Set system name
location..... Set system location
contact..... Set system contact name
getcommunity... Set GET community
setcommunity... Set SET community
trapcommunity.. Set TRAP community of specified trap
trapip..... Set TRAP IP address of specified trap
```

User can use the command to configure the following items for SNMP operation.

a. *Name of the switch* with “**name**” sub-command.
b. *Location of the switch* with “**location**” sub-command.
c. *Contact for the switch* with “**contact**” sub-command.
d. *GET Community string* with “**getcommunity**” sub-command
e. *SET Community string* with “**setcommunity**” sub-command.
f. *TRAP Community string* with “**trapcommunity**” sub-command.
g. *TRAP IP Address* with “**tapip**” sub-command.

Its syntax is . . .

```
>set snmp trapip
Syntax: set snmp trapip [id] [ip address]
```

This switch supports five trap IP addresses. The [id] is 1~5 for the five trap IP addresses. For example, “set snmp trapip 1 192.168.1.10”.

For example, “set snmp name ABC location AAA-1F contact Jack” command will set these SNMP information to switch.

9.13 **set trunk** command

This switch supports Port-based trunk and Mac-Based trunk function. For Port-based trunk operation, the traffic is assigned based on the physical port assignment. For example, the traffic from Port 5 could be assigned to cable 1 in the trunk. This command is used to configure the Port-based trunk

function. The trunk groups are disabled and null trunk groups default. Users can use this command to configure trunk function of the switch.

Its syntax is . . .

```
>set trunk
Syntax     : Set trunk enable
Description: Enable trunk function.

Syntax     : Set trunk disable
Description: Disable trunk function.

Syntax     : Set trunk [+/-] [port#] [trunk#]
Examples   : Set trunk +1+5-7 1
Description: Add port 1,5 to trunk group 1 and
             remove port 7 from trunk group 1
```

a. **enable** and **disable** sub-commands are used to enable/disable trunk function of the switch.
b. **set trunk [+/-] [port#] [trunk#]** is sub-command to add/remove ports to trunk groups.

9.14 **set mactrunk** command

This switch supports Port-based trunk and Mac-Based trunk function. For Mac-based trunk operation, the traffic is assigned based on the Mac address of the traffic. This command is used to configure the Mac-based trunk function. The trunk groups are disabled and null trunk groups default. Users can use this command to configure Mac-based trunk function of the switch.

Its syntax is . . .

```
>set mactrunk
[Syntax]set mactrunk [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
enable..... Enable MAC-based trunk
disable..... Disable MAC-based trunk
hash..... Set port trunking hash index selection
giga..... Set Giga port trunk

Syntax     : Set mactrunk [+/-] [port#] [trunk#]
Examples   : Set mactrunk +1+5-7 1
Description: Add port 1,5 to MAC-based trunk group 1 and
             remove port 7 from MAC-based trunk group 1
```

The **hash** sub-command is used to select the index Mac address is source address, destination address or both.

Its syntax is . . .

```
>set mactrunk hash
Syntax: Set mactrunk hash [DA | SA | ALL]!
[DA] : use hast destination address to generate index!
[SA] : use hast source address to generate index!
[ALL]: use hast (DA^SA) to generate index!
```

The **giga** sub-command is used to select the trunk with gigabit ports.

Its syntax is . . .

>set mactrunk giga
Syntax: Set mactrunk giga [disable | 0 | 1 | 2]!
[disable] : Disable Giga port trunking!
[0 | 1 | 2]: Specify Giga group id to enable Giga port trunking!
0= Port 9/G1,10/G2
Note: 9/G1 means the Port# is 9 and it is the 1st gigabit port.

9.15 **set trunkforward** command

This command is used to assign traffic of physical ports for port-based trunk function.

Its syntax is . . .

>set trunkforward
Syntax : Set trunkforward auto
Description: Set forwarding map assignment to be automatic.

Syntax : Set trunkforward manual
Description: Set forwarding map assignment to be manual.

Syntax : Set trunkforward [+/-] [port#] [trunk-port#]
Examples : Set trunkforward +1+5-7 1
Description: Add port 1,5 to port-based trunk port 1 and
remove port 7 from port-based trunk port 1

The physical port traffic assignment could be assigned automatically by the switch or manually. As the above example, the network traffic from user ports Port 1,5 will go through Port 1 if the traffic will go through the trunk. (Port 1 is one of the ports in the trunk group.) And network traffic from user port Port 7 is removed from Port 1.

9.16 **set vlan** command

This command is used to configure port-based VLAN.

Its syntax is . . .

>set vlan
Syntax : Set VLAN enable
Description: Enable VLAN function.

Syntax : Set VLAN disable
Description: Disable VLAN function.

Syntax : Set VLAN [+port#/-port#] [vlan#]
Examples : Set vlan +1+2+3+4+5-7 1
Description: Add port 1,2,3,4,5 to VLAN 1 and
remove port 7 from VLAN 1

As the above example, it adds Port 1,2,3,4,5 to VLAN 1 and removes Port 7 from VLAN 1. For these ports that are not assigned to any VLAN groups, the switch will put them to the internal default VLAN.

9.17 **set 1qvlan** command

This command is used to configure 802.1Q VLAN.

Its syntax is . . .

>set 1qvlan

[Command List]
enable..... Set 802.1Q enabled.
disable..... Set 802.1Q disabled.
membermap..... Set 802.1Q VLAN table membership.
tag..... Set 802.1Q VLAN table port tagged/untagged.
default_tag.... Set 802.1Q default tag of specified port.
newprimap..... Enable remap priority, and set new priority.
frame_cntl..... To change frame's priority, VID or both.
vtable..... Set drop or flood if VLAN table is not found.
ifilter..... Set ingress filter.
drop_n_1q..... Drop the non 1Q frame of specified port.

enable, **disable**: enable/disable 802.1Q VLAN function
membermap: add/remove port to/from a 802.1Q VLAN.
Its syntax is . . .
>set 1qvlan membermap
Syntax: set 1qvlan membermap [vid=#] [+|- port]
vid: 1 ~ 4094
tag: configure ports in a 802.1Q VLAN being tagged or untagged port.
Its syntax is . . .
>set 1qvlan tag
Syntax: set 1qvlan tag [vid=#] [+|- port]
vid: 1 ~ 4094
"+" is for tag port and "-" is for untag port.
For example, "set 1qvlan tag vid 5 + 12" will set Port 12 in VLAN 5 as a tagged port. "set 1qvlan tag vid 5 - 11" will set Port 11 in VLAN 5 as a untagged port.
default_tag: configure the VLAN ID and priority of port for tag adding. The assigned VLAN ID and priority will be used for tag adding.
Its syntax is . . .
>set 1qvlan default_tag
Syntax : set 1q_vlan default_tag [port=#] [pvid=#] [pri=#]
Port ID : 1 ~ 10, or manage
Pvid : 1 ~ 4094
Pri : 0 ~ 7
Examples: set 1q_vlan default_tag port=manage pvid=1 pri=2
: set 1q_vlan default_tag port=1 pvid=1 pri=2
newprimap: for new priority mapping of tag operation. The priority value in tag will be mapped to the new value.
Its syntax is . . .
>set 1qvlan newprimap
Syntax: set 1qvlan newprimap [enable | disable] [oldpri-newpri]
oldpri: 0 ~ 7
newpri: 0 ~ 7
For example, "set 1qvlan newprimap enable 3-5" will enable the priority re-mapping operation and Priority 3 will be mapped to Priority 5.
frame_cntl: for re-assign VLAN ID and Priority value function. You can change the VLAN ID and/or Priority value of a packet to the default tag setting.
Its syntax is . . .
>set 1qvlan frame_cntl
Syntax: set 1q_vlan frame_cntl [none | vid | priority | vid_priority]

none: is for “no change”.
vid: is for “change VLAN ID”.
priority is for “change priority”.
vid_priority: is for “vid_priority”.
Note: If “vtable” is set to “drop” or “ifilter” is set to “on”, the VLAN ID change may be no effect because the packet with different VLAN ID could be dropped first.
vtable: for the process of packet with unknown VLAN ID in tag (i.e. the VLAN is not in current VLAN table.) The packet could be dropped or flooded to every port.
Its syntax is . . .
>set 1qvlan vtable
Syntax: set 1qvlan vtable [drop | flood]
ifilter: for VLAN ingress filter function. The VLAN filtering operation will be processed at ingress port or not.
Its syntax is . . .
>set 1qvlan ifilter
Syntax: set 1qvlan ifilter [on | off]
drop_n_1q: for the process of untagged (not 802.1Q) packet. The untagged packets could be forwarded or dropped.
Its syntax . . .
>set 1qvlan drop_n_1q
Syntax: set 1qvlan drop_n_1q [port=#] [drop | nodrop]
Port ID: 1 ~ 10

9.18 **set dot1x** command
This command is used to configure the 802.1x function of the switch.
Its syntax is . . .
>set dot1x
[Syntax]set dot1x [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
enable..... Set 802.1x enable
disable..... Set 802.1x disable
transparent.... Set 802.1x transparent
re_au..... Set 802.1x Re-authentication
reauthtime..... Set 802.1x Re-authentication Timeout Period
reauthcnt..... Set 802.1x Re-authentication Max Count
reqcnt..... Set 802.1x Max Request Count
sertime..... Set 802.1x Server Timeout Period
supptime..... Set 802.1x Supplicant Timeout Period
quiettime..... Set 802.1x Quiet Timeout Period
txtime..... Set 802.1x Tx Timeout Period
rsip..... Set Radius Server Address
authport..... Set Authenticate Port of Radius Server
shkey..... Set 802.1x Security Key
portauth..... Set 802.1x port auth mode

enable sub-commands is used to enable 802.1x authentication function.
disable sub-command is used to disable 802.1x function.

transparent sub-command is used to set the operation of 802.1x function to transparent mode. In this mode, the switch will forward 802.1x packets directly.
re_au sub-command is used to enable the re-authentication function of the switch. When the re-authentication time is up, the switch will start the re-authentication process.
reauthtime sub-command is used to set the timeout period of the re-authentication process.
reauthcnt sub-command is used to set max count for re-authentication request in the re-authentication process. If the max count is met, it will become un-authentication state. The valid value is 1~10.
reqcnt sub-command is used to set max request timeout count between the switch and RADIUS server before authentication fail. The valid value is 1~10.
sertime sub-command is used to set the request timeout value between the switch and RADIUS server. The valid value is 0~65535.
supptime sub-command is used to set the timeout value between the switch and users (called "supplicant" in 802.1x) after first identification. The valid value is 0~65535.
quiettime sub-command is used to set the quiet time value between the switch and the user before next authentication process when authentication fail.
txtime sub-command is used to set the timeout value for the identification request from the switch to users. The request will be re-tried until the ***reauthcnt*** is met. After that, authentication fail message will be sent. The valid value is 0~65535.
rsip sub-command is used to set the IP address of RADIUS server.
authport sub-command is used to set the handshaking port number between the switch and RADIUS server. It could be different for different RADIUS servers.
shkey sub-command is used to set the security key between the switch and RADIUS server.
portauth sub-command is used to set the authentication mode for a physical port. Its syntax is . . .
set dot1x portauth [port#] [auto|fa|fu|no]

- auto: the authentication mode of the port depending on the authentication result of the port
- fa (force-authenticated): will force the port always being authentication successful in 802.1x process and the real authentication result will be ignored.
- fu (force-unauthenticated): will force the port always being authentication unsuccessful in 802.1x process and the real authentication result will be ignored.
- none: 802.1x function will not be executed on the port, i.e. disabled on the port.

Note: This switch supports MD5, TLS and PEAP authentication types.

9.19 **set security** command

This command is used to set the Mac address security mode of physical port. If it is enabled and ports are set to “accept”, only the users with the static Mac address on the ports can access network through these ports.
Its syntax is . . .

```
>set security
[Syntax]set security [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
disable..... Set MAC Security disable
enable..... Set MAC Security enable
port..... Set MAC Security port mode
```

disable sub-command is used to disable the Mac security function.
enable sub-command is used to enable the Mac security function. Because this function cannot work with 802.1x function at the same time, you will be asked to disable 802.1x function first when you enable this function. (If 802.1x function is already disabled, you can enable this function directly.)
port sub-command is used to set the Mac security function on each port. Its syntax is . . .

```
>set security port
Port number is missing!
Syntax: set security port [port#] [no|accept]
```

no is used to disabled this function on the port.
accept is used to set this port to accept static Mac address only.

For examples, “set security port 1 accept” will set Port 1 to accept the users with the static Mac addresses configured on Port 1 only. Please refer to “set arl” command for static address setting. (You can find the Mac addresses learned on each port by “show arl” command.)

Note: Here is an *Application Note* for Mac address filter-in function.
It needs two conditions for Mac address filter-in function working.
1. The port security mode is set to “Accept”.
2. Static Mac address is assigned on Port (for example, Mac 1 on Port 1).
In this case, only Mac 1 can access network through Port 1. But there is also a limitation for Mac 1 - it can access network through Port 1 only because it is a static fixed address on Port 1.

9.20 **set sta** command
This command is used to configure spanning tree protocol of the switch.
Its syntax is . . .

```
>set sta
[Command List]
?..... Help commands
help..... Help commands
enable..... Enable Spanning Tree function
disable..... Disable Spanning Tree function
bridge..... Set Spanning Tree bridge configuration
port..... Set Spanning Tree port configuration
```

a. **set sta ?** and **set sta help** commands will show the sub-command list

b. **set sta enable** and **set sta disable** commands will enable/disable spanning tree function of the switch.

c. **set sta bridge** command is used to configure for the switch.

Its syntax is . . .

```
>set sta bridge
[Syntax]set sta bridge [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
priority..... Set bridge priority.
hello..... Set bridge hello time
age..... Set bridge maximum age
delay..... Set bridge forward delay time
```

priority (0~65535) : Bridge priority is for selecting the root device, root port, and designated port. The device with the highest priority (lowest value) becomes the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device.

hello (0~65535) : the period to send the spanning tree maintenance packet if the switch is the root of the spanning tree. Default is 2 seconds.

age (6~40) : the spanning tree aging time if no spanning tree maintenance packet is received. It will cause the spanning tree to re-create. Default is 20 seconds.

delay (4~30): the maximum waiting time before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.

d. **set sta port** command is used to configure for ports of the switch.

Its syntax is . . .

```
>set sta port 1
[Syntax]set sta port [port#] [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
priority..... Set port priority.
cost..... Set port path cost
```

priority (0~255) : If the path cost for all ports on a switch are the same, the port with the highest priority (lowest value) will be forwarded when looping happens. If more than one port have the same highest priority, the port with lowest port number will be forwarded.

cost (1~65535) : It is used to determine the best path between devices if looping happens. Lower values will be forwarded and should be assigned to ports with fast connections. Higher values will be blocked and should be assigned to ports with slow connections. The suggestion values are 100(50~600) for 10M, 19(10~60) for 100M and 4(3~10) for 1000M connections.

9.21 **set http** command

This command is used to enable/disable the http function of the switch. Because hacker or worm/virus (like ColdRed) often attacks http server, this command is provided to disable http to prevent it. (If this switch is installed in public Internet without any firewall protection, we suggest users to disable the http interface and use Telnet or SNMP instead.)

Its syntax is . . .

```
>set http
Syntax     : Set http enable
Description: Enable http protocol function.
Syntax     : Set http disable
Description: Disable http protocol function.
```

10. **show** command

This command is used to show configurations of the switch. Here is the sub-command for showing different configuration.

```
>show
[Command List]
?..... Help commands
help..... Help commands
age..... Show Switch age
idle..... Show idle time for CLI session
arl..... Show ARL table
cfg..... Show system configuration
net..... Show network configuration
igmp..... Show IGMP configuration
mirror..... Show mirror configuration
automode..... Show Auto mode setting
port..... Show switch port configuration
qos..... Show QoS configuration
snmp..... Show snmp configuration
trunk..... Show all TRUNK groups with their members
version..... Show firmware version
vlan..... Show all VLAN groups with their members
1qvlan..... Show all 802.1Q setting
dot1x..... Show 802.1x Protocol Status
security..... Show MAC Security Configuration
sta..... Show Spanning Tree setting
http..... Show HTTP Protocol setting
```

10.1 **show ?** and **show help** commands will show the sub-command list.

10.2 **show age** command will show the aging time setting of the switch.

10.3 **show idle** command will show the period for auto-logout when console interface is idle.

10.4 **show arl** command will show Mac address setting content in ARL table. It has four sub-commands.

```
all..... List all addresses in table (both static and dynamic addresses)
static..... List static addresses in ARL table
dynamic..... List dynamic addresses in ARL table
```

10.5 **show cfg** command will show model name and Mac address of the switch. For example,

```
>sh cfg
[System Configuration]
Model   Name : Intelligent Switch
MAC  Address : 00:C0:F6:50:36:6E
```

10.6 **show net** command will show IP address/Mask address/Gateway address setting of the switch. For example,

```
>show net
[eth0] Network Configuration:
IP Address: 192.168.1.250
Netmask   : 255.255.255.0
Gateway   : 192.168.1.254
```

10.7 **show igmp** command will show the setting and status of IGMP function. For example,

```
>sh igmp
[IGMP Configuration]
IGMP Switch     : Disabled
IGMP Router Port: 2
Total Groups    : 0
```

"Router Port" is the port connecting to the active IGMP device.
"Total Groups" is the IP multicast group number learned by the switch.

10.8 **show mirror** command will show mirror function configuration of the switch. For example,

```
>sh mirror
[Mirror Configuration]
Mirror Switch:Disabled
Capture port :1
Ingress DIV=1     Mode=ALL  MAC=00-00-00-00-00-00
       Port List:
Egress  DIV=1     Mode=ALL  MAC=00-00-00-00-00-00
       Port List:
```

"DIV=n" is capture one packet for every n packets.
"Mode" is for capturing filter – all packets, some source Mac address or some destination Mac address.

10.9 **show automode** command will show current auto mode setting for port configuration. It could be **Auto Negotiation** and **Auto Detect**.
For *Auto Negotiation* mode, the switch will do auto-negotiation ON/OFF when the auto mode of port is enabled/disabled. But the Auto-MDIX function will also be disabled when the auto-negotiation function of port is OFF.
For *Auto Detect* mode, the switch will always keep auto-negotiation function ON but just modify its attribution if the auto mode of port is disabled. The Auto-MDIX function will be always enabled in this mode.

For applications, you should select *Auto Detect* mode if the connected device is auto-negotiation enabled. And you can select *Auto Negotiation* mode if the connected device is auto-negotiation disabled.
For most applications, *Auto Detect* mode is OK.

10.10 **show port** command will show status and configuration of each switch port. For example,

```
>show port
[Port Configuration]
Port Name      Status   Admin     AN    Speed   Duplex   Flow
 1   YYY       DOWN    Enabled   OFF   10      Half     Disabled
 2   Port 2    DOWN    Enabled   ON    10      Half     Disabled
 3   Port 3    DOWN    Enabled   ON    10      Half     Disabled
 4   Port 4    DOWN    Enabled   ON    10      Half     Disabled
 5   Port 5    UP      Enabled   ON    100     Full     Disabled
 6   Port 6    DOWN    Enabled   ON    10      Half     Disabled
 7   Port 7    DOWN    Enabled   ON    10      Half     Disabled
 8   Port 8    DOWN    Enabled   ON    10      Half     Disabled
 9   Port 9    DOWN    Enabled   ON    1000    Full     Disabled
10   Port 10   DOWN    Enabled   ON    10      Half     Disabled
```

10.11 **show qos** command will show QoS configuration of the switch. For example,

```
>sh qos
 [QoS Configuration]
 Qos setting    : Disabled
 802.1p Priority: 0
 HQ Weight      : 4
 LQ Weight      : 1
 Port  Priority  Port  Priority  Port  Priority  Port  Priority
 [ 1]  Low       [ 2]  Low       [ 3]  Low       [ 4]  Low
 [ 5]  Low       [ 6]  Low       [ 7]  Low       [ 8]  Low
 [ 9]  Low       [10]  Low
```

"802.1p Priority" is the threshold of 0~7 for high/low priority queues.
"HQ/LQ Weight " is the traffic weighting between the high/low priority queues.
"Port Priority" is port-based priority setting.

10.12 **show snmp** command will show SNMP configuration of the switch. For example,

```
>show snmp
[SNMP Configuration]
Object ID     : 1.3.6.1.4.1.655.6.3
System up Time: 29138 (seconds)
System Name   :
Location      :
Contact name  :
Get Community : public
Set Community : private
[Trap Community]
ID  Status    Community    IP Address
1   Disabled  public       0.0.0.0
```

```
2  Disabled  public        0.0.0.0
3  Disabled  public        0.0.0.0
4  Disabled  public        0.0.0.0
5  Disabled  public        0.0.0.0
```

The “Status” is the trap operation status of each trap IP address.

10.13 **show trunk** command will show trunk configuration of the switch. For example,

```
>show trunk
[Trunk Group Setting]
Trunk Setting: MAC-based Trunk
Hash Index   : DA ^ SA
Giga trunk group  : Disabled

[TRUNK]  [Port List]
=======  ====================================
 [ 1]        1 2  3
```

“Trunk Setting” could be Port-based or Mac-based. For Port-based trunk, the traffic assignment between trunk cables is based on physical port. For Mac-based trunk, the traffic assignment between trunk cables is based on Mac address of the traffic.

10.14 **show version** command will show firmware version of the switch
For example,

```
>sh version
Firmware Version: 2.20.03 (built at Oct  1 2004 12:51:44)
```

10.15 **show vlan** command will show current port-based VLAN setting. For example,

```
>sh vlan
VLAN Setting:  Enabled

[VLAN]  [Port List]
======  ====================================
 [ 1]       1  2  3
```

10.16 **show 1qvlan** command will show 802.1Q VLAN setting and status. For example,

```
>show 1qvlan
[802.1Q Configuration]
802.1Q setting            : Enabled
Frame Control             : No change
Ingress filter          : Filter Off
Vtable not found          : Flood
VLAN Lookup               : MAC Address and VID
Remap New Priority        : Disabled

Drop none 1Q frame:
Port  Drop   Port  Drop   Port  Drop   Port  Drop
1     NO     2     NO     3     NO     4     NO
5     NO     6     NO     7     NO     8     NO
```

```
9     NO     10     NO

New Priority Map:
old-new    old-new    old-new    old-new
 0-0         1-0         2-0         3-0
 4-0         5-0         6-0         7-0

Default Tag:
Management Port Default tag Priority=0, PVID=1
Port  PVID  Pri   Port  PVID  Pri   Port  PVID  Pri   Port  PVID  Pri
1     1     0     2     1     0     3     1     0     4     1     0
5     1     0     6     1     0     7     1     0     8     1     0
9     1     0     10    1     0

[VID]      [Port List]
======  ====================================
 1         1[U]  2[U]  3[U]  4[U]  5[U]  6[U]
           7[U]  8[U]  9[U] 10[U]
```

"Frame Control" is for changing VLAN ID and Priority of a packet to the ingress port default tag setting.
"Ingress Filter" is for doing VLAN filtering at ingress port.
"Vtable not found" is for dropping or flooding the packets with unknown VLAN ID.
"Remap New Priority" is for mapping a priority value to another priority value.
"Default Tag" is the default tag setting of each port for tag adding.

10.17 **show dot1x** command will show current 802.1x status and settings.
Its syntax is . . .

```
>show dot1x
Syntax: show dot1x [config|radius|port]
            config : show 802.1x protocol status
            radius : show radius server status
             port  : show ALL ports status
```

For example,

```
>show dot1x config
[802.1x Configuration]
802.1x Protocol                : Disabled
Re-authentication              : Disabled
Re-authentication Timeout Period : 3600
Re-authentication Max Count    : 2
Max Request Count              : 2
Server Timeout Period          : 30
Supplicant Timeout Period      : 30
Quiet Timeout Period           : 60
Tx Timeout Period              : 30

>show dot1x radius
[Redius Server Configuration Menu]
Redius Server IP Address  : 192.168.1.222
Redius Server Port Number : 1812
```

```
Security Key            : 12345678

>show dot1x port
802.1X Port Authentication Configuration Menu
PORT      Status      Auth.Mode
================================
 1          -          FA
 2          -          FA
 3          -          FA
 4          -          FA
 5          -          FA
 6          -          FA
 7          -          FA
 8          -          FA
 9          -          FA
10          -          FA
```

The Auth. Mode could be Auto, FA(Forced Authenticated), FU(Forced Unauthenticated) and No(No 802.1x function).

10.18 **show security** command will show current Mac address security mode for port.
Its syntax is . . .

```
>show security
[MAC Security Configuration]
 MAC Security Setting : Disabled
============================================================
  Port              Security Control
============================================================
    1                 No Security
    2                 No Security
    3                 No Security
    4                 No Security
    5                 No Security
    6                 No Security
    7                 No Security
    8                 No Security
    9                 No Security
   10                 No Security
============================================================
```

The “Security Control” could be *No*, *Accept* modes. “No” is for no Mac address security. “Accept” is for accept static Mac addresses only.

10.19 **show sta** command will show spanning tree configuration of the switch. For example,

```
> sh sta
[Spanning Tree Configuration]
SPT Setting         : Disabled
Bridge Priority     : 32768
Bridge Hello Time   : 2
Bridge Max Age      : 20
Bridge Forward Delay: 15
Port  Priority  Path Cost  Link Delay  State
```

```
==================================================
1    128    19        ON        None
2    128    19        ON        None
3    128    19        ON        None
4    128    19        ON        None
5    128    19        ON        None
6    128    19        ON        None
7    128    19        ON        None
8    128    19        ON        None
9    128    19        ON        None
10   128    19        ON        None
```

It shows the Bridge and Port spanning tree configuration.

10.20 **show http** command will show http enable/disable state. For example,

```
>show http
[HTTP Protocol Setting]
HTTP Setting: Enabled
```

11. **Upgrade** command

This switch supports firmware or configuration upgrade with TFTP protocol. This command is used to upgrade firmware or configuration to the switch.
Its syntax is . . .

```
>upgrade
Syntax: upgrade [firmware | config] ip filename
```

ip is the IP address of TFTP server.
filename is the upgrade file name in the TFTP server.

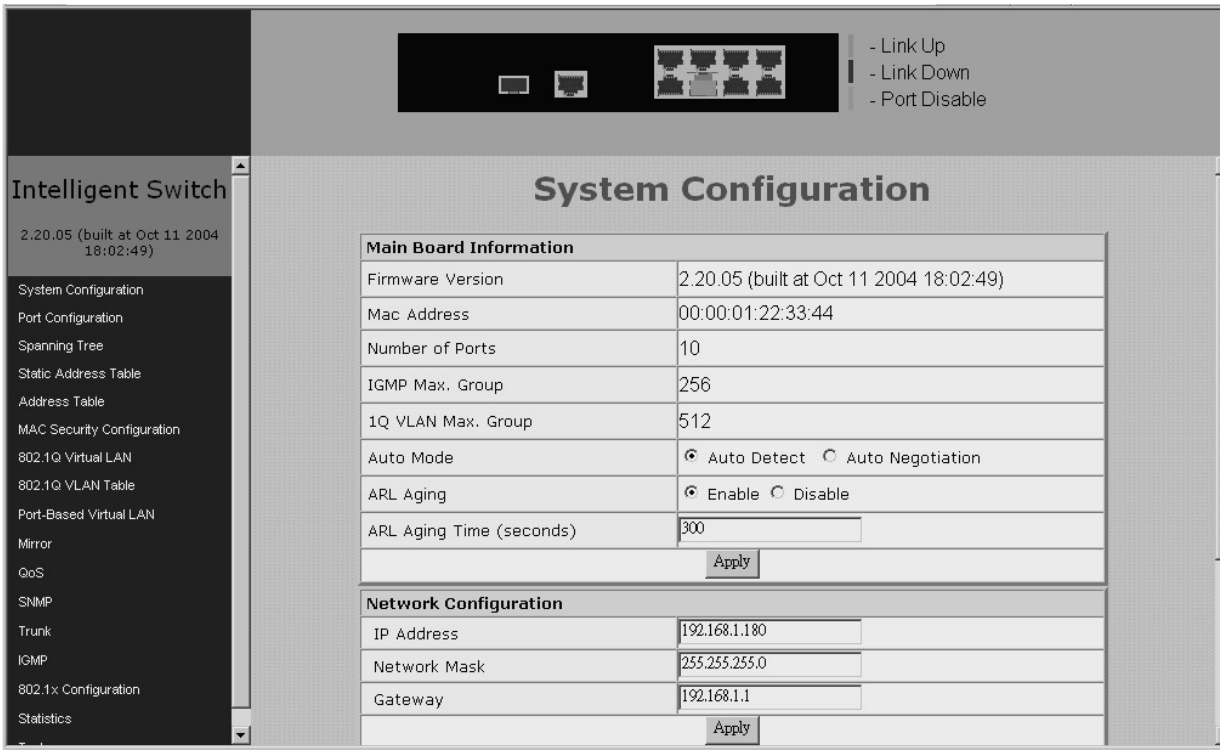
For example, “upgrade config 192.168.1.80 abcd” command will load file “abcd” from TFTP server 192.168.1.80 as its configuration setting.

6.3 Management with Http Connection

Users can manage the switch with Http Web Browser connection. Before http connection, IP address configuration of the switch should be done first.

Please follow the instruction in Section 6.2 to complete the console connection and use "**show net**" command to check IP address of the switch first. If users want to change the IP address of the switch, use "**set eth0 ip xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx gateway xxx.xxx.xxx.xxx**" command to modify the IP address of the switch.

After IP address configuration done and the switch is connected to network, users can start Http connection by entering IP address of the switch to the web address line in Web Browser. A login screen will be prompted for user name and password. The default user name and password is "**admin**" / "**123456**".. Then the management homepage will appear.

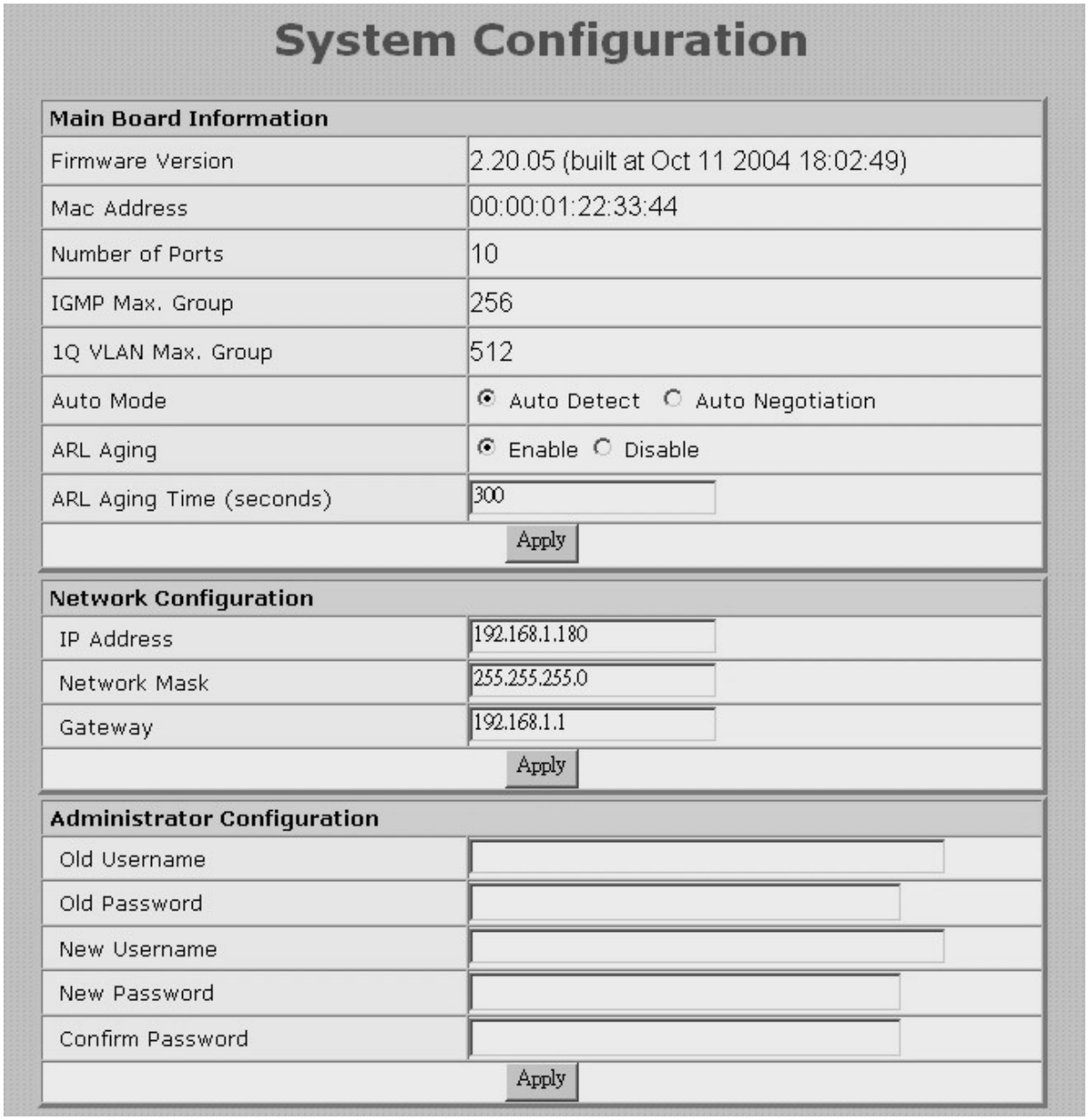


Left part of the homepage is a function list. Users can select one of them for status monitoring or switch configuration.

Upper part of the homepage is the link status of the switch. Three different colors are used to show different status of ports – Link Up, Link Down and Port Disable.

Middle part of homepage is the main operation area for each function.

1. System Configuration



"System Configuration" is the homepage of the switch.

Users can find firmware version and Mac address of the switch in this page. And users can configure the following items in this page.

a. **Auto Mode** : You can select the auto function of connection port here.

For *Auto Negotiation* mode, the switch will do auto-negotiation ON/OFF when the auto mode of port is enabled/disabled. But the Auto-MDIX function will also be disabled when the auto-negotiation function of port is OFF.

For *Auto Detect* mode, the switch will always keep auto-negotiation function ON but just modify its attribution if the auto mode of port is disabled. The Auto-MDIX function will be always enabled in this mode.

For applications, you should select *Auto Detect* mode if the connected device is auto-negotiation enabled. And you can select *Auto Negotiation* mode if the connected device is auto-negotiation disabled.

For most applications, *Auto Detect* mode is OK.

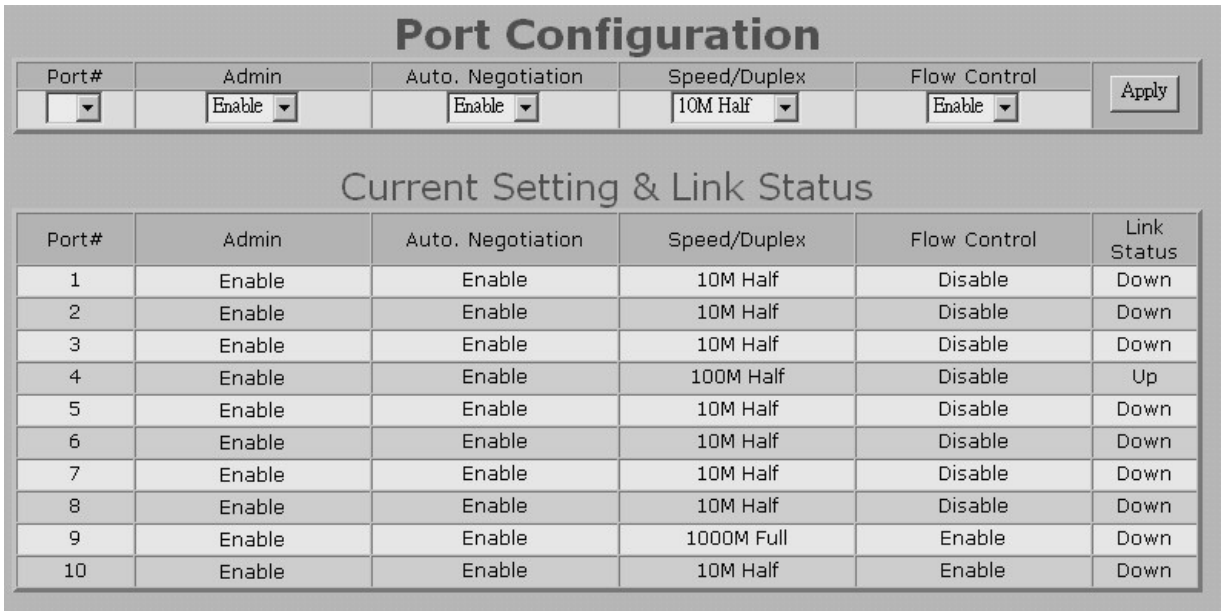
b. **ARL Aging** : Users can enable/disable the aging operation of the switch and modify the aging time here. (Default is 300 seconds.)

c. **Network Configuration** : Here is for IP address configuration of the switch.

d. **Administrator Configuration** : This is for network administrator to change his/her username and password. (Default is admin/123456.)

If any modification, click [Apply] to activate the new setting.

2. Port Configuration



Port Configuration

Port#	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	
	Enable	Enable	10M Half	Enable	Apply

Current Setting & Link Status

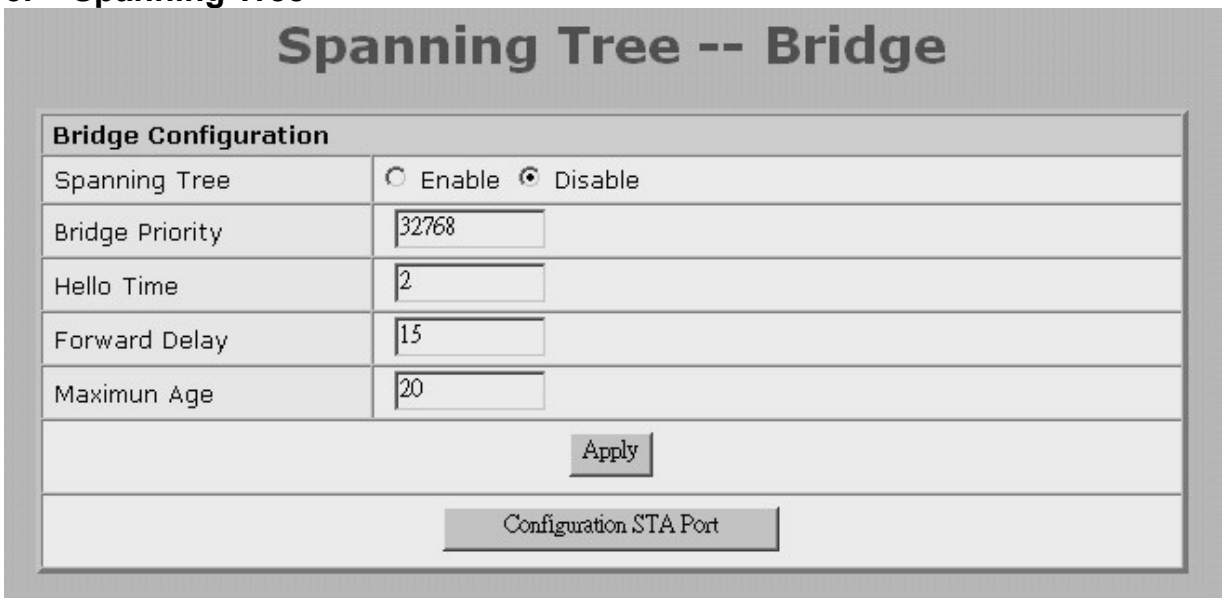
Port#	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	Link Status
1	Enable	Enable	10M Half	Disable	Down
2	Enable	Enable	10M Half	Disable	Down
3	Enable	Enable	10M Half	Disable	Down
4	Enable	Enable	100M Half	Disable	Up
5	Enable	Enable	10M Half	Disable	Down
6	Enable	Enable	10M Half	Disable	Down
7	Enable	Enable	10M Half	Disable	Down
8	Enable	Enable	10M Half	Disable	Down
9	Enable	Enable	1000M Full	Enable	Down
10	Enable	Enable	10M Half	Enable	Down

You can find link status and port status here.

In this page, you can enable/disable port connection function in “Admin.” and configure their operation mode in “Auto”, “Speed/Duplex” and “Flow Control”. If “Auto” is enabled, the setting of “Speed” and “Duplex” will be ignored.

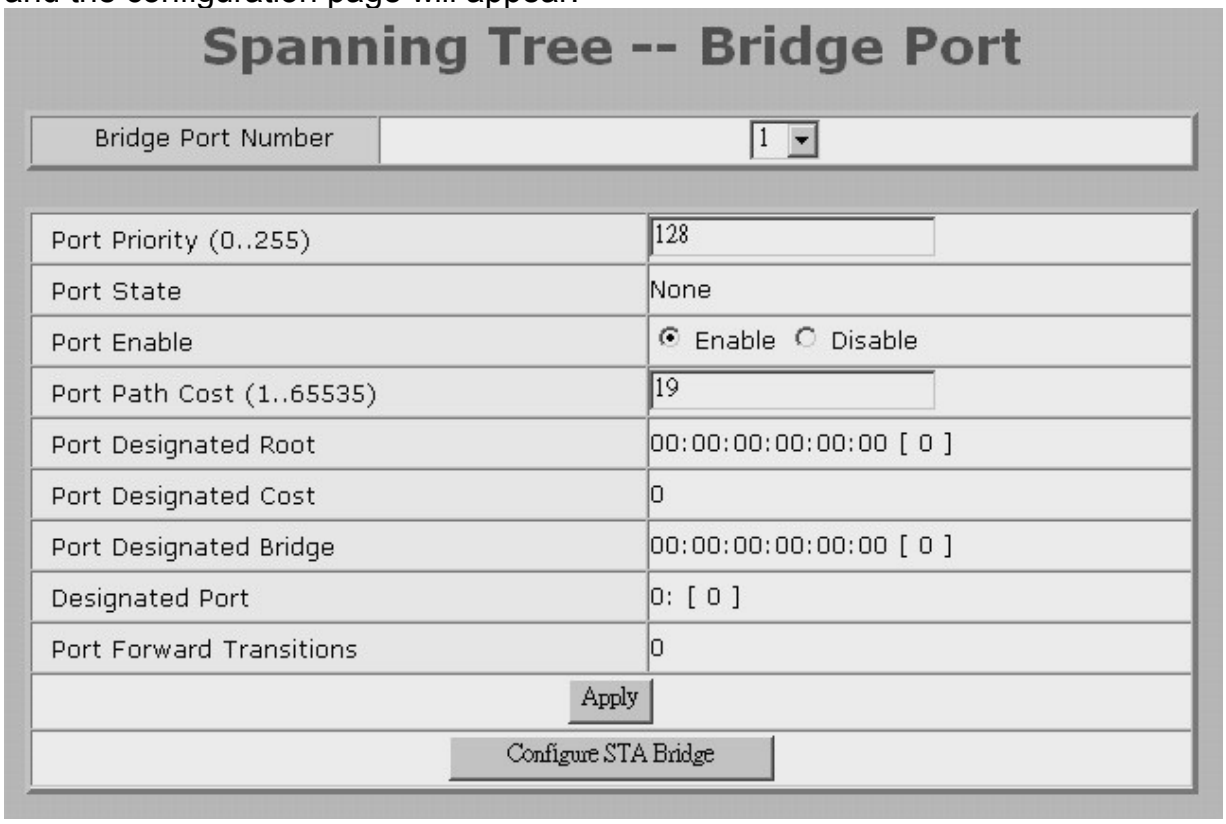
Click [Apply] after any modification.

3. Spanning Tree



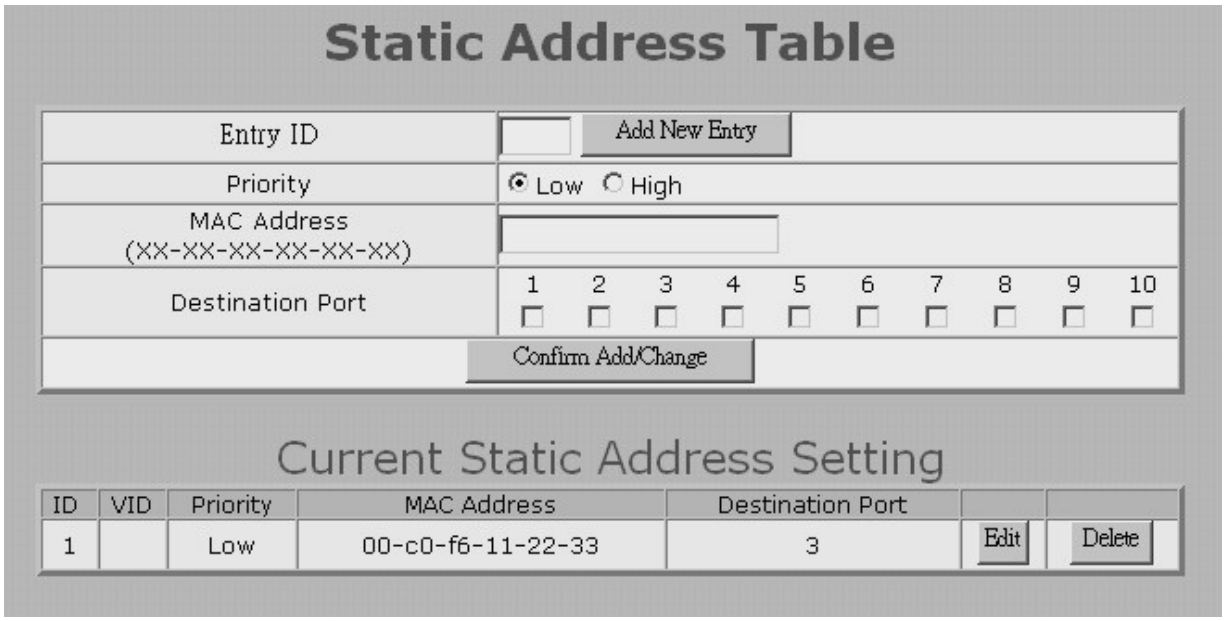
In the page, users can enable/disable spanning tree function and configure the bridge parameters. Please refer to **9.20 of Section 6.2** for the details of these parameters. Press [Apply] after any modification.

Configuring port parameters for spanning tree, press [Configuration STA Port] and the configuration page will appear.



Users can select a port number and check its spanning tree status. Users can also modify these parameters. Please refer to **9.20 of Section 6.2** for the details of these parameters. Press [Apply] after any modification.

4. Static Address Table



This switch supports static Mac address assignment on port.

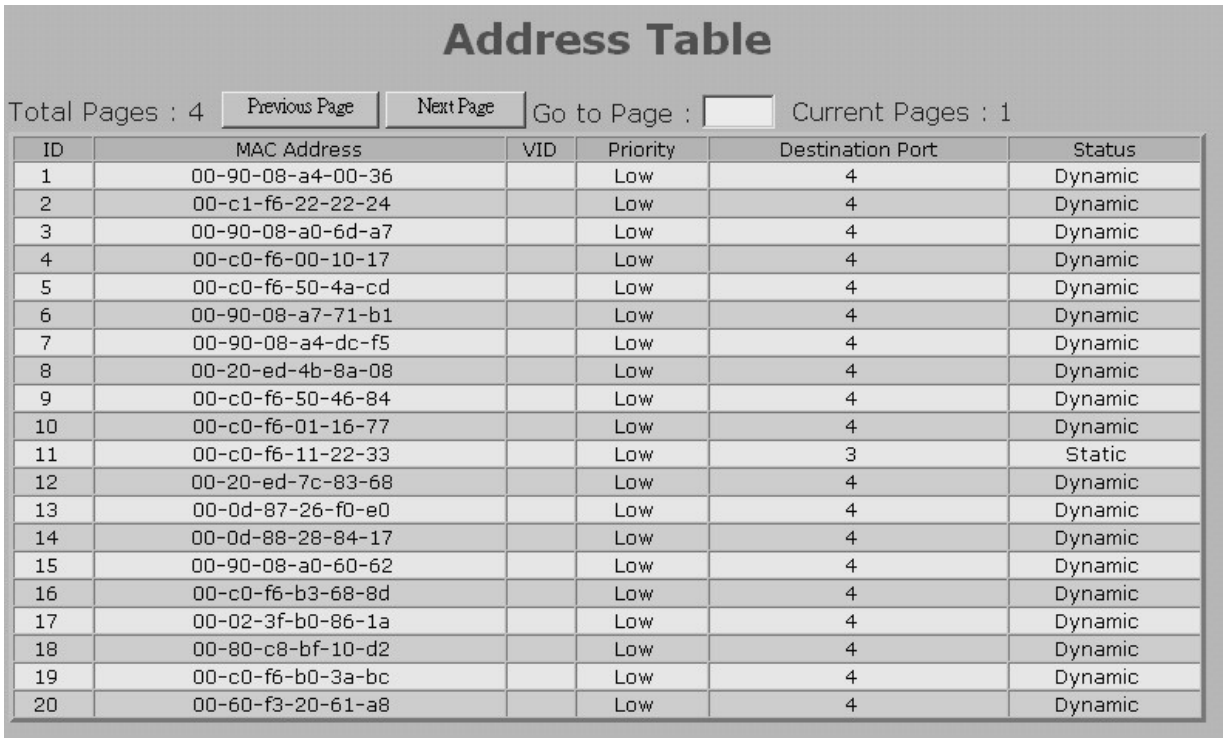
This switch will not age out these static Mac addresses. But there is a limitation for these static Mac addresses - *they are allowed to work on the assigned port only because they are static fixed on the assignment port*.

For Mac address access limit application -
If Mac Security function is enabled and the port is set to *Accept* mode, only the static addresses assigned on the port will be accepted by the port for network access. With this function, you can limit the users that can access network through the switch.

You can find the Mac addresses learned on each port in **Address Table** page. The table is useful for static Mac address assignment.

If you want to delete an entry in the static Mac address table, click [Delete] button of the entry and the static Mac address will be removed from the table.

5. Address Table



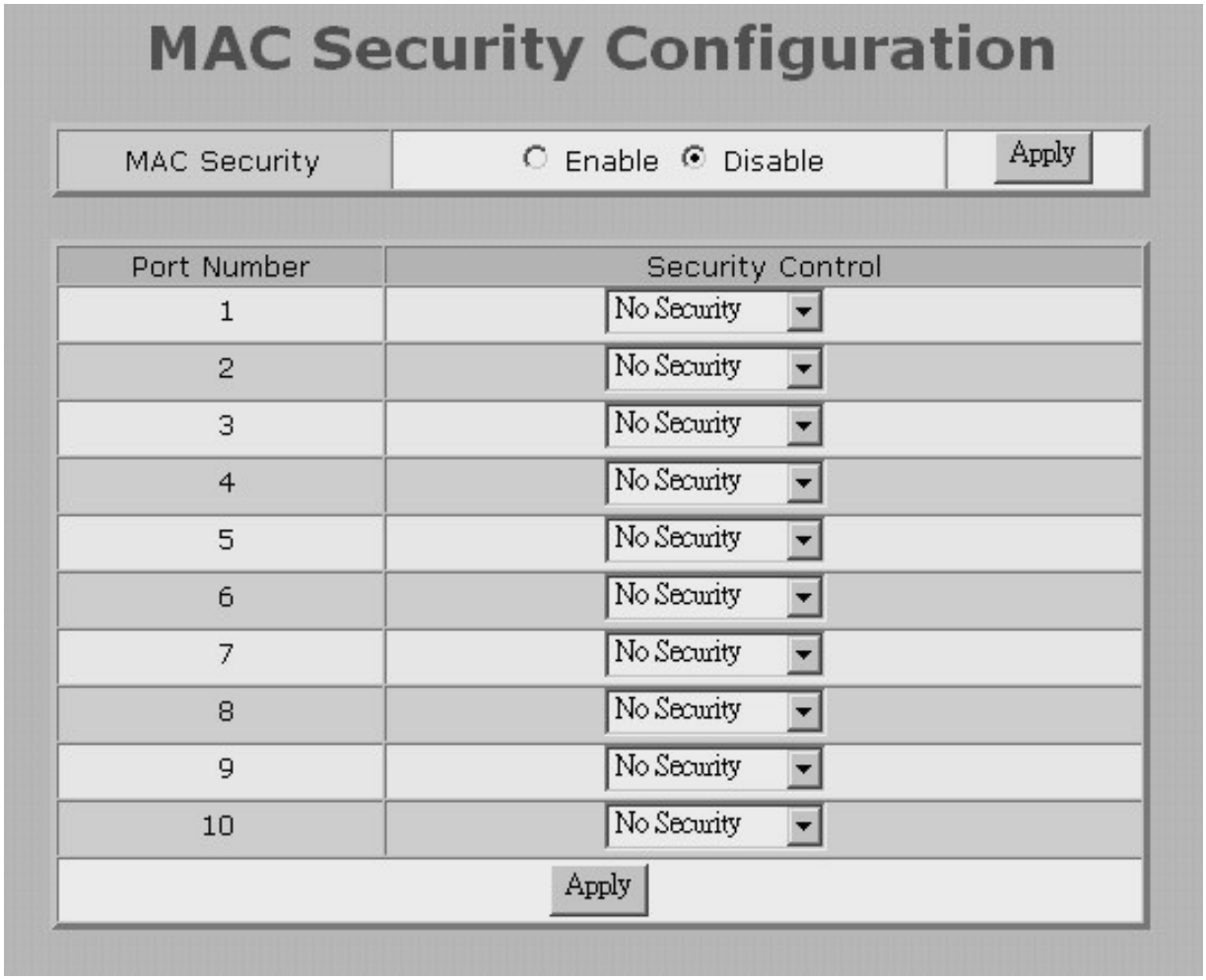
ID	MAC Address	VID	Priority	Destination Port	Status
1	00-90-08-a4-00-36		Low	4	Dynamic
2	00-c1-f6-22-22-24		Low	4	Dynamic
3	00-90-08-a0-6d-a7		Low	4	Dynamic
4	00-c0-f6-00-10-17		Low	4	Dynamic
5	00-c0-f6-50-4a-cd		Low	4	Dynamic
6	00-90-08-a7-71-b1		Low	4	Dynamic
7	00-90-08-a4-dc-f5		Low	4	Dynamic
8	00-20-ed-4b-8a-08		Low	4	Dynamic
9	00-c0-f6-50-46-84		Low	4	Dynamic
10	00-c0-f6-01-16-77		Low	4	Dynamic
11	00-c0-f6-11-22-33		Low	3	Static
12	00-20-ed-7c-83-68		Low	4	Dynamic
13	00-0d-87-26-f0-e0		Low	4	Dynamic
14	00-0d-88-28-84-17		Low	4	Dynamic
15	00-90-08-a0-60-62		Low	4	Dynamic
16	00-c0-f6-b3-68-8d		Low	4	Dynamic
17	00-02-3f-b0-86-1a		Low	4	Dynamic
18	00-80-c8-bf-10-d2		Low	4	Dynamic
19	00-c0-f6-b0-3a-bc		Low	4	Dynamic
20	00-60-f3-20-61-a8		Low	4	Dynamic

This page will show the Mac addresses learn by the switch.

This information is useful for network administrator to check the user connection status.

Note: Because of *aging time operation* of switch, wrong Mac addresses could be found in the Mac Address Table sometimes. These wrong Mac addresses are the machines that had ever accessed to the port and the switch learns them into the learning table. The switch will clear them when the aging time is up. Users can shorten the aging time and refresh the page when they want to get the correct Mac address table content. Then, recover the aging time when the correct Mac address table content is got.

6. Mac Security Configuration



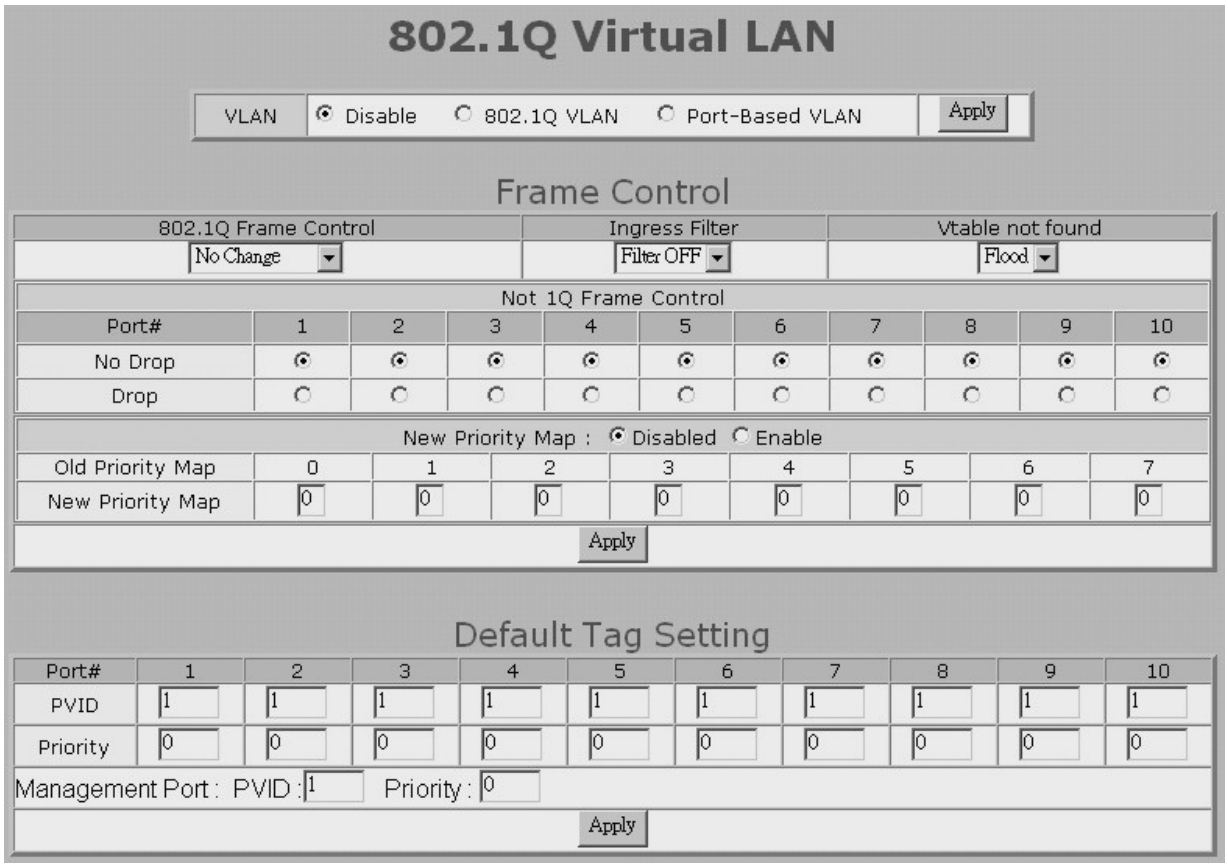
This function is used to limit the users that can access network through the switch. If this function is enabled and the port is set to *Accept* mode, only those users with the static Mac addresses can be accepted by the port for network access. (You can create the static address list in the **Static Address Table** page.)

Because this function cannot work with 802.1x function at the same time, you will be asked to disable 802.1x function first if you want to enable this function. (If 802.1x function is not enabled, you can enable this function directly.)

Steps to setup Mac access limit function:

1. Disable 802.1x function first.
2. Enable Mac Security function.
3. Set the port that will be applied for user limit to *Accept* mode.
4. Assign the Mac addresses that will be allowed for network access to Static Mac Address table. (You can refer to the Address Table for the Mac address learned by the switch.)

7. 802.1Q Virtual LAN


802.1Q Virtual LAN
VLAN
Disable
802.1Q VLAN
Port-Based VLAN
Apply
Frame Control
802.1Q Frame Control
No Change
Ingress Filter
Filter OFF
Vtable not found
Flood
Not 1Q Frame Control
Port# 1 2 3 4 5 6 7 8 9 10
No Drop
Drop
New Priority Map : Disabled Enable
Old Priority Map 0 1 2 3 4 5 6 7
New Priority Map 0 0 0 0 0 0 0 0
Apply
Default Tag Setting
Port# 1 2 3 4 5 6 7 8 9 10
PVID 1 1 1 1 1 1 1 1 1 1
Priority 0 0 0 0 0 0 0 0 0 0
Management Port : PVID : 1 Priority : 0
Apply

This web page is for 802.1Q VLAN setting. The operation of 802.1Q VLAN is based on the "tag" in a packet. A tag contains a 12-bit VLAN ID and 3-bit priority information.

A packet with tag inside is called tagged packet and a packet without tag inside is called untagged packet. Packet sent from tag port will always be tagged packet and packet sent from untag port will always be untagged packet. The process and translation of tagged packet and untagged packet is configured in the 802.1Q VLAN.

You can assign a default tag setting for each physical port. The setting includes VLAN ID and priority for the port. If untagged packet is received and forwarded to a tagged port, the default setting will be used for tag adding operation.

VLAN

For the VLAN function, you can select "Disable", "Port-based VLAN" or "802.1Q VLAN". If "Port-based VLAN" is selected, you can configure the VLAN at **Port-based Virtual LAN** page. If "802.1Q VLAN" is selected, you can configure the VLAN at **802.1Q VLAN Table** page.

Frame Control

[802.1Q Frame Control]

The switch can change VLAN ID and Priority setting in a packet. You can select [No Change]/[Change Priority]/[Change VID]/[Change Both] in the Frame Control function. If any modification is requested, the default tag value will be used to replace the VLAN ID or Priority in the packet.

Note: If [Ingress Filter] is set to “ON” or [Vtable not found] is set to “Drop”, the VLAN ID modification may be no effect because the packet with different VLAN ID is dropped first.

[Ingress Filter]
This function can enable the VLAN filtering function at ingress port instead of egress port. If this is ON, the packet with different VLAN ID will be filtered out at ingress port instead of egress port.

[Vtable not found]
A packet with an unknown VLAN ID (not in the VLAN table of the switch) could be dropped or flooded to every port. You can configure it in this function.

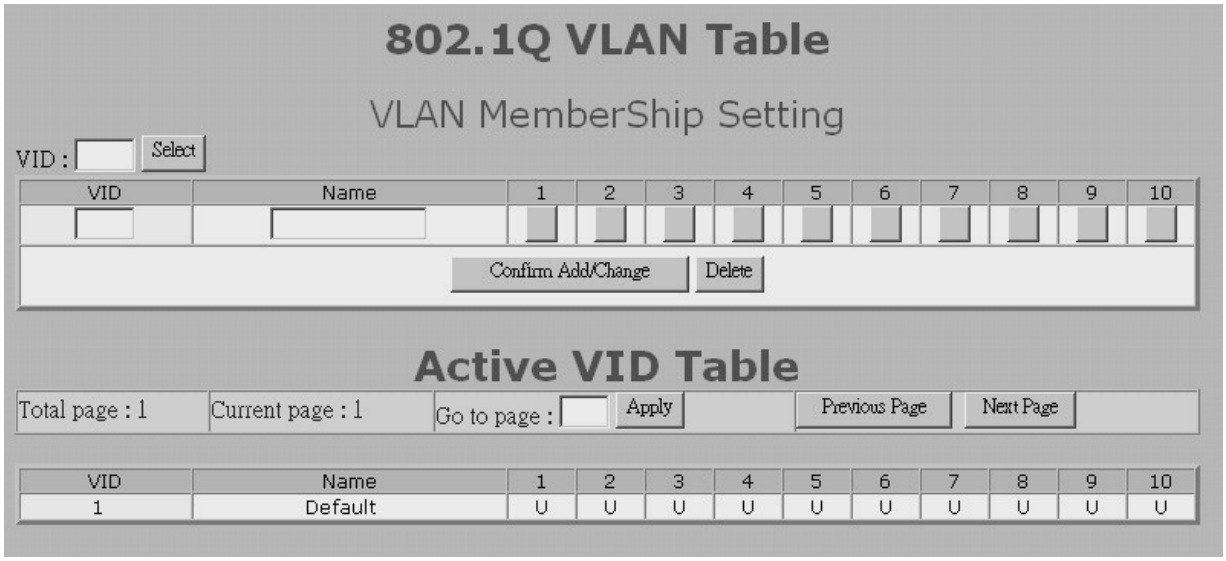
[Not 1Q Frame Control]
If untagged packet is received, it should be dropped or forwarded. You can configure it for each physical port here.

[New Priority Map]
This function can re-map the priority operation. For example, you can map Priority 3 to Priority 5 and all the packets with Priority 3 will works as they had Priority 5.

Default Tag Setting
[VID and Priority for Port 1~10]
It is the default tag setting for each physical port. These values will be used for tag adding or frame control.

[VID and Priority for Management Port]
The management port is the internal port for management CPU. You can put the internal CPU to different VLAN for management security application – only the users in the same VLAN of the Management Port can do in-band management of the switch.

8. 802.1Q Table



802.1Q VLAN Table

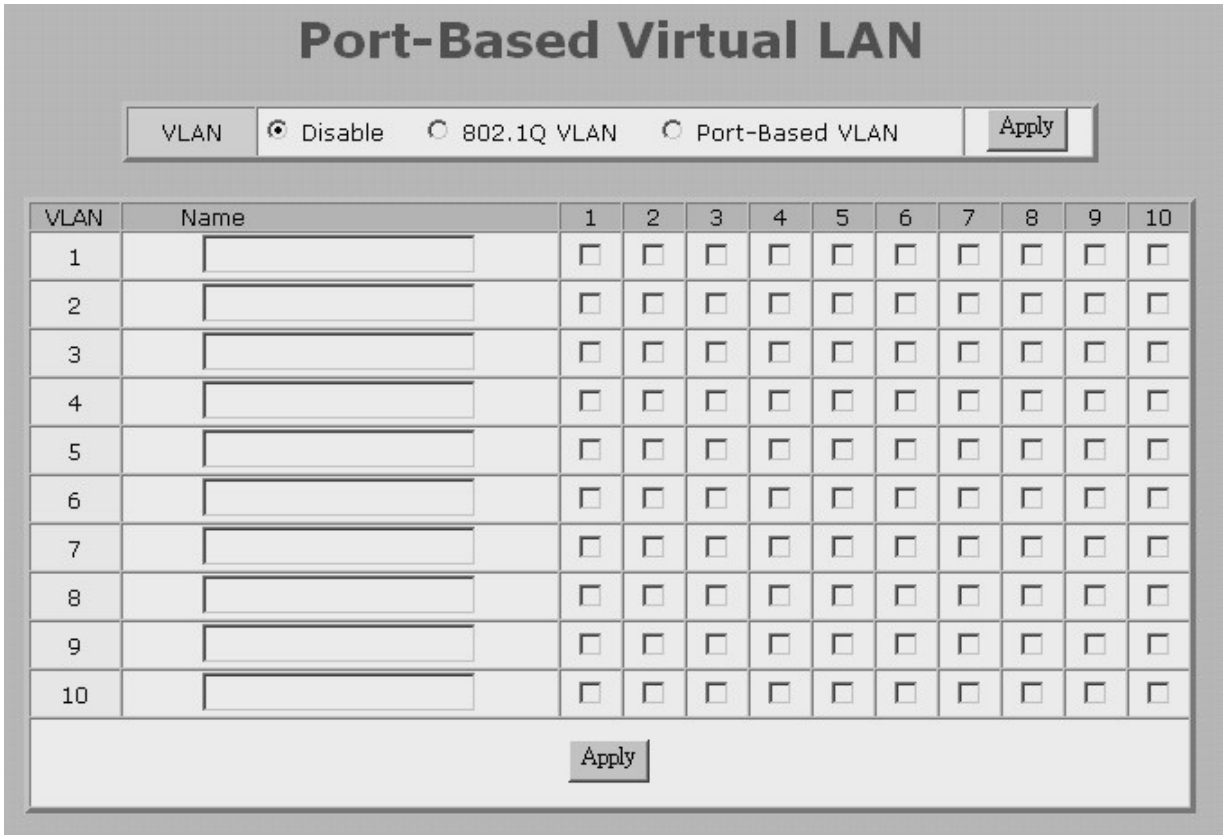
This function is used to configure the static VLAN setting. Follow the steps to complete a VLAN configuration.

1. Input a VLAN ID in “VID” and click [Select].
2. Input a VLAN name in “Name”.
3. Click the port to add or remove the port to/from the VLAN. “T” means tagged port. “U” means untagged port. Blank means not in the VLAN.
4. Click [Confirm Add/Change] to complete the setting.

Active VID Table

This table shows the list of 802.1Q VLAN configuration.

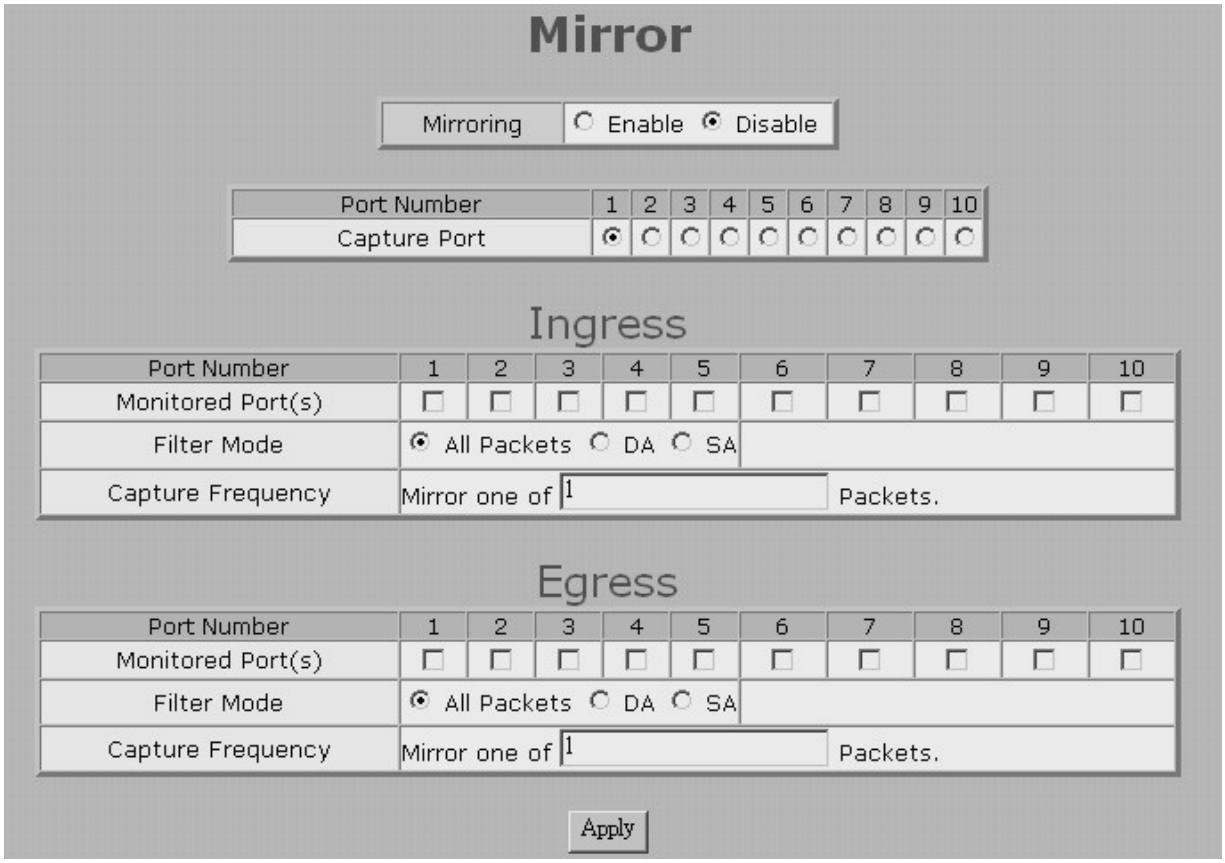
9. Port-based Virtual LAN



This function is used to configure Port-based VLAN.

1. Select VLAN to “Port-base VLAN” and click [Apply].
2. Give a name for the VLAN.
3. Mark the ports for the VLAN.
4. Click [Apply] to activate the setting.

10. Mirror

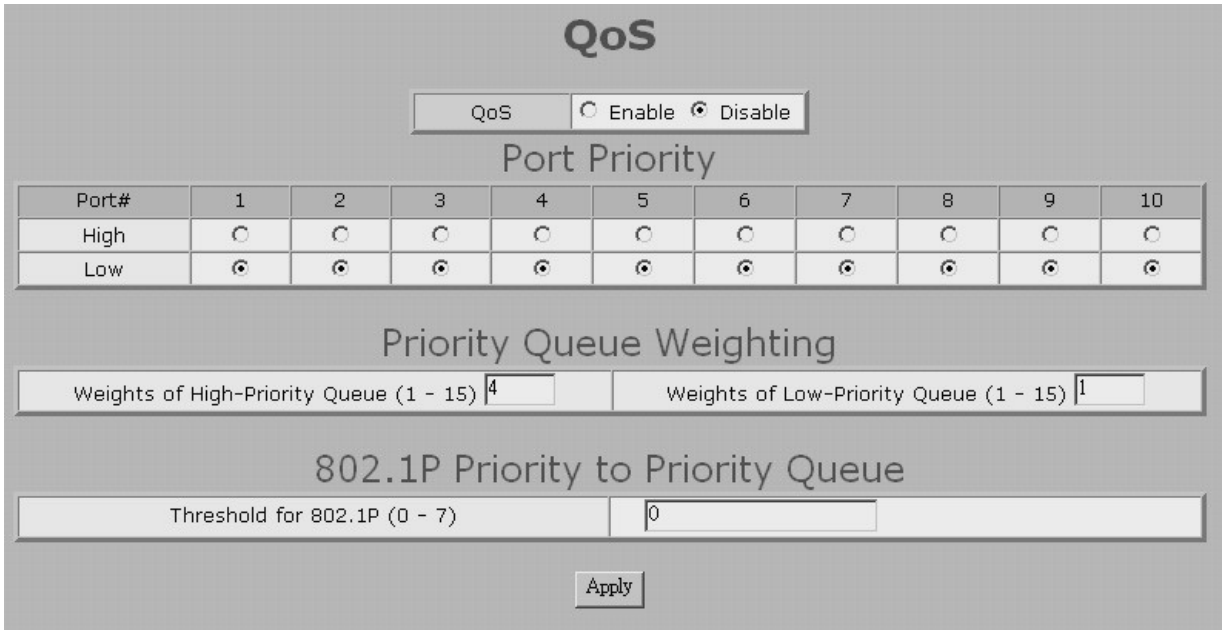


Follow the steps to configure Mirror function.

1. Enable Mirroring first.
2. Select the capture port.
3. Select the monitored port from Ingress or Egress table – depending on the traffic direction.
4. Select the capture mode – All packets or for some special DA/SA address. If DA/SA is selected, enter the special Mac address in “xx-xx-xx-xx-xx-xx” format.
5. Select the capture frequency.
6. Press [Apply] button.

If users want to disable Mirror function, select Disable and click [Apply].

11. QoS

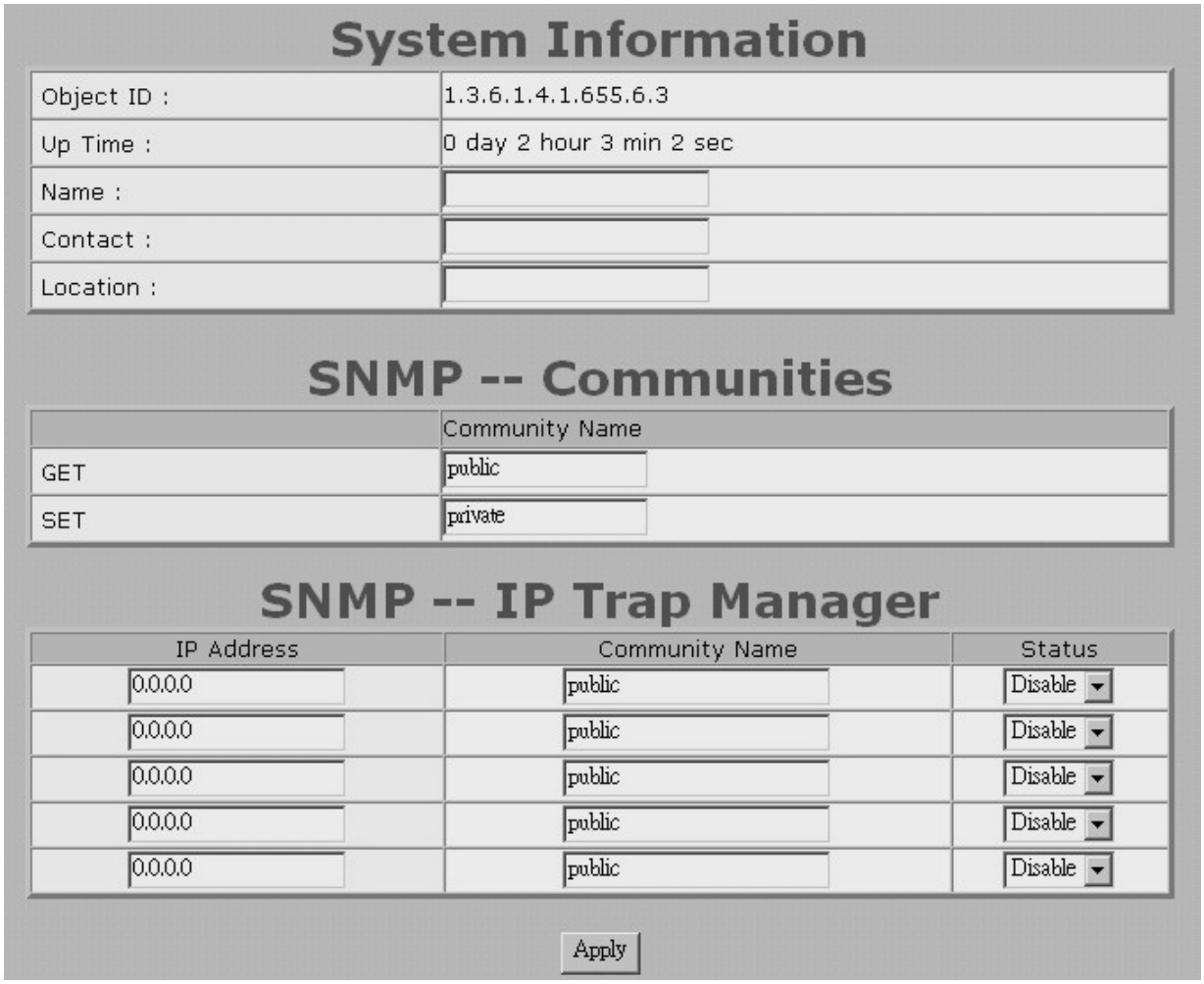


This switch supports two priority queues on each port for QoS operation. Follow the steps to configure QoS function.

1. Enable QoS first.
2. If port-based priority is used, select ports for High and Low priorities.
3. Set the weight of traffic rate for high priority queue and low priority queue.
4. For 802.1P tagged packet, its priority value is 0 ~ 7. Set the threshold of the priority value for high priority queue.
5. Click [Apply] to activate the setting.

If you want to disable QoS operation, select Disable and click [Apply] button.

12. SNMP



In this page, you can find and configure the system information. You can also configure GET/SET/Trap Community Name and the IP address for trap operation. Then users can manage this switch with these settings from SNMP management program.

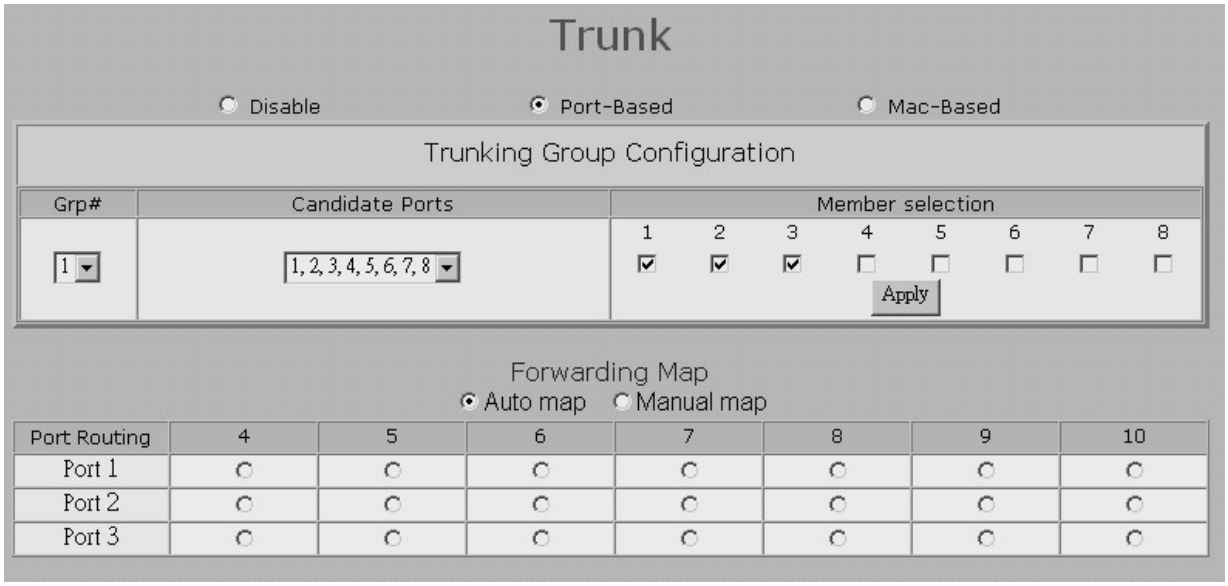
13. Trunk

This switch supports Port-based Trunk and Mac-based Trunk function.

For Port-based Trunk, the traffic assignment between trunk cables is based on physical port – e.g. the traffic from Port 5 will go through cable 1 and the traffic from Port 12 will go through cable 2. The traffic assignment could be automatic by the switch or manual by administrator.

For Mac-based Trunk, the traffic assignment between trunk cables is based on the Mac address of the traffic – e.g. the traffic with Mac address 00-00-e2-98-11-29 will go through cable 1 and the traffic with Mac address 00-00-e2-98-11-A3 will go through cable 2. The switch does the traffic assignment based on the Mac address.

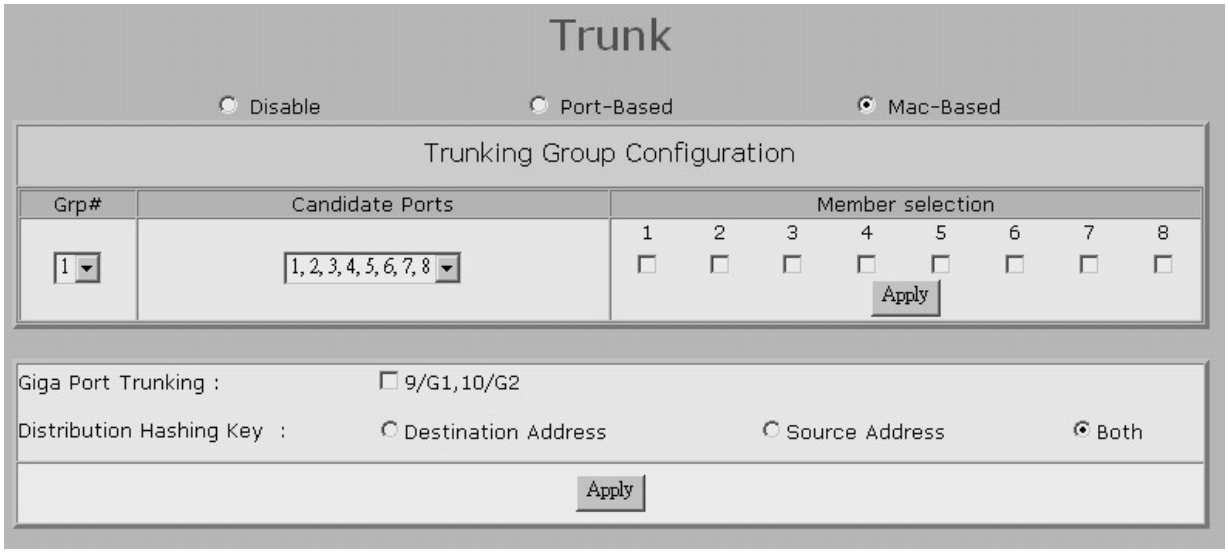
[For Port-based Trunk]



This switch supports 4 trunk groups and they are null by default. If you want to use port-based trunk function, follow the steps to configure it.

a. Select “Port-based” first.
b. Assign ports to the trunk. Then click [Apply]. The trunk is created.
c. Select “Auto Map” or “Manual Map” for traffic assignment.
d. If “Manual Map”, assign user-port to trunk-port and the traffic from the user-port will go through the trunk cable of the trunk-port.
e. If you want to remove ports from trunk, unmark the port and click [Apply]. The selected port will be removed from trunk groups.

[For Mac-based Trunk]



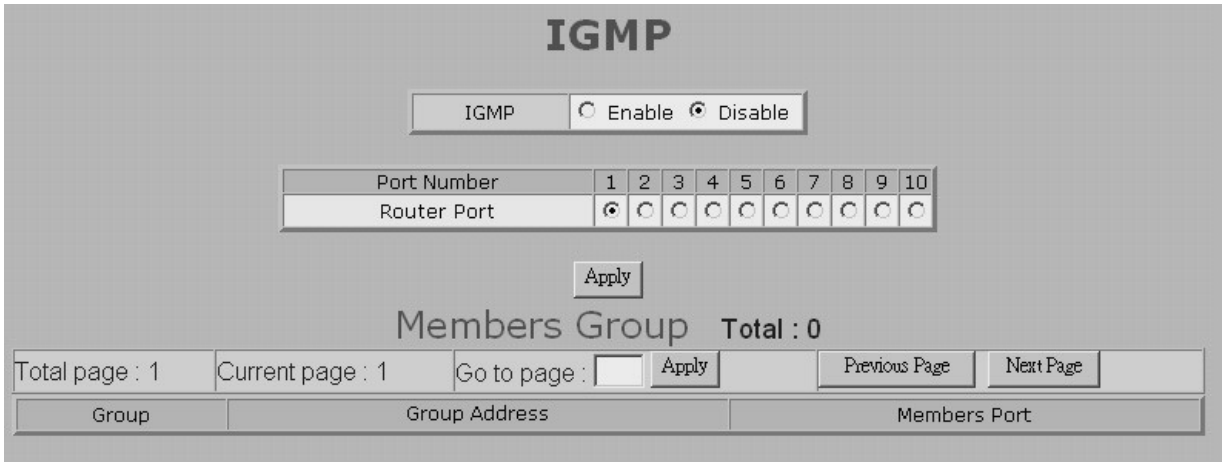
This switch supports 4 trunk groups and they are null by default. If users want to use Mac-based trunk function, follow the steps to configure it.

a. Select “Mac-based” first.
b. Assign ports to the trunk. Then click [Apply]. The trunk is created.
c. Select the Mac address key is source or destination or both.
d. If you want to use gigabit ports for trunk, select from “Gigabit Trunk”. (9/G1 means Port 9 and its is the first Gigabit port.)

If you want to remove ports from trunk, unmark the port and click [Apply]. The selected port will be removed from trunk groups.

[Disable Trunk]
If you want to disable trunk function, select “Disable” and click [Apply] button. The switch will clear the Trunk configuration.

14. IGMP

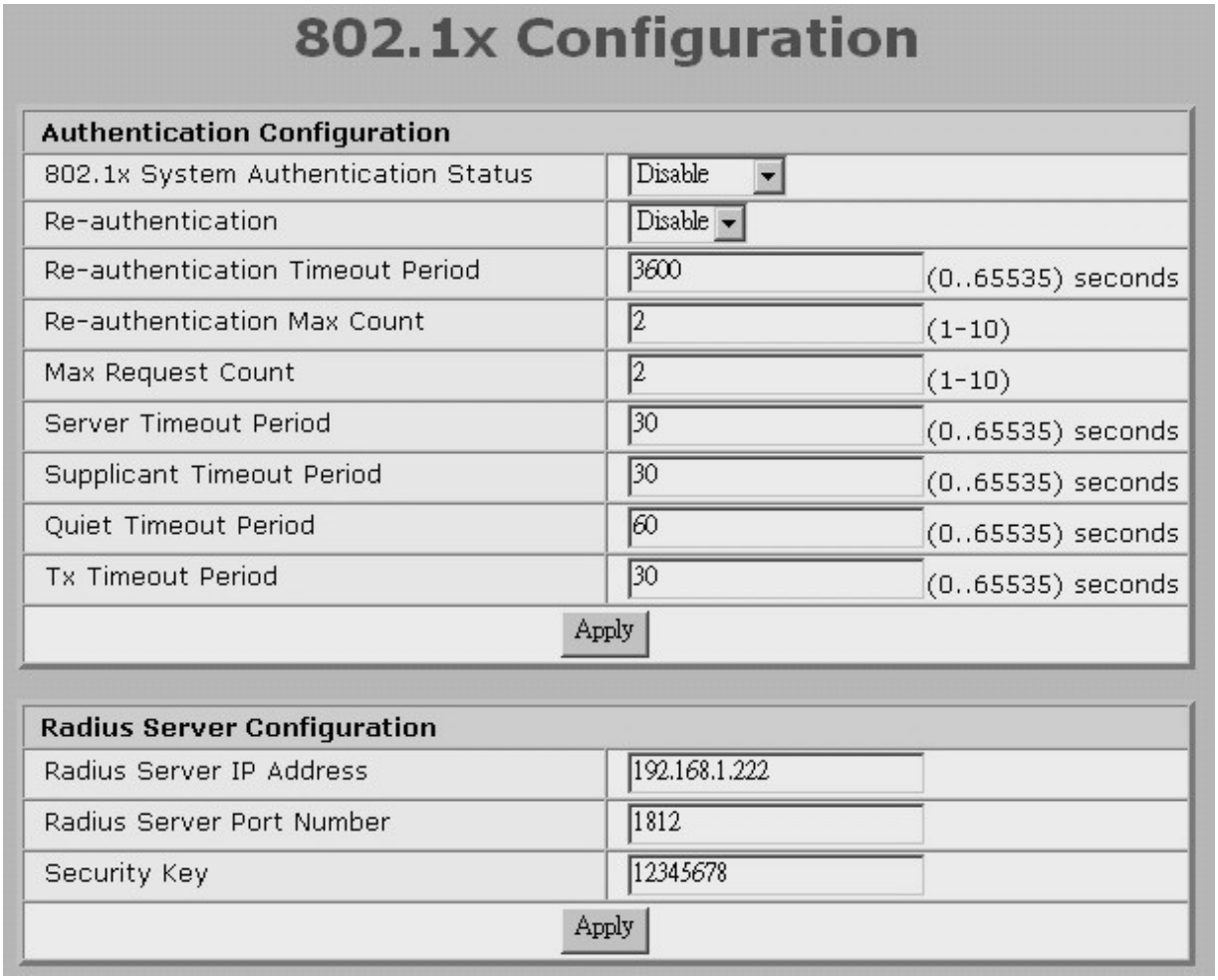


This switch supports IP multicast function with IGMP snooping operation.

Follow the steps to complete the setting.
1. Enable IGMP first.
2. Select “Router Port” – the port connecting to the IGMP active device.
3. Click [Apply].

The learned IP multicast groups is shown in “Members Group”.

15. 802.1x Configuration



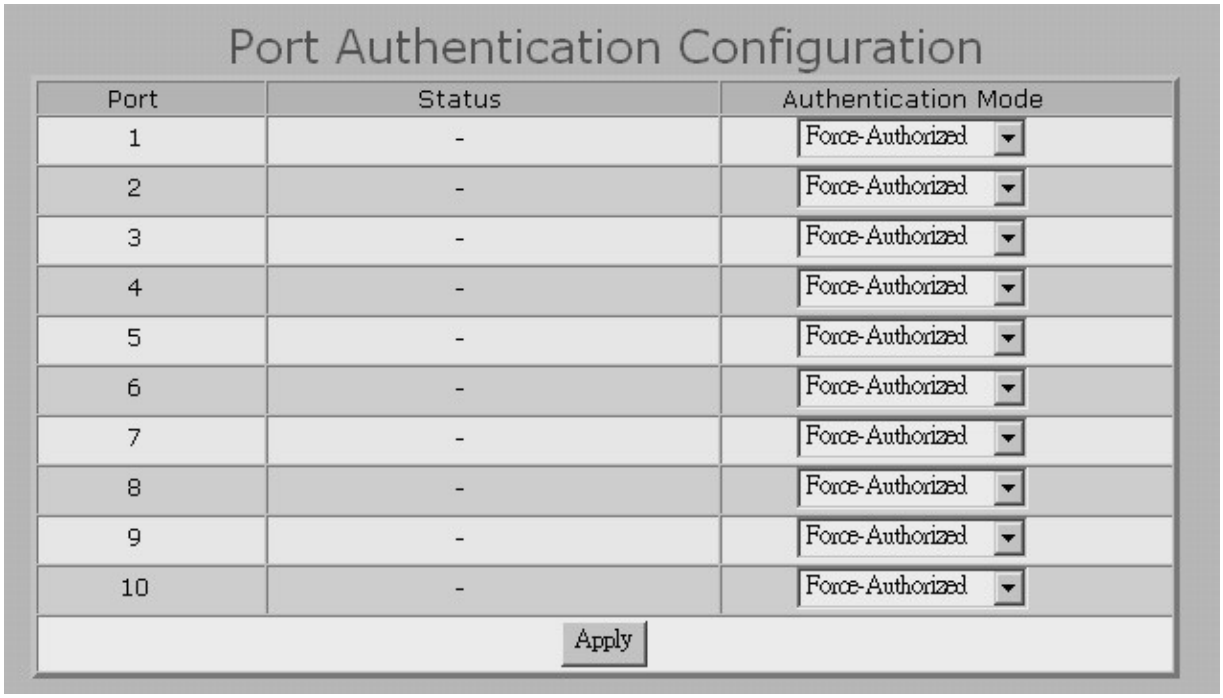
The 802.1x function can limit the port access for authentication users only. It needs a RADIUS server for the authentication process and the switch acts as an authenticator.

The function here is for 802.1x function configuration.

1. 802.1x System Authentication Status: [Enable/Disable/Transparent]
   Enable: enable 802.1x function in authentication mode
   Disable: disable 802.1x function
   Transparent: forwarding 802.1x packets directly
   (Note: Because 802.1x and Mac security function cannot work at the same time, you could be asked to disable Mac security function first when you enable 802.1x.)
2. Re-authentication (enable/disable), Timeout Period and Max Count:
   The re-authentication function will re-authenticate users after the timeout period. The Max Count is the maximum re-try count between the switch and users before authentication fail.
3. Max Request Count and Server Timeout Period:
   The Server Timeout Period is the timeout period for the request between the switch and RADIUS server.

The Max Request Count is the maximum re-try count between the switch and RADIUS server before authentication fail.

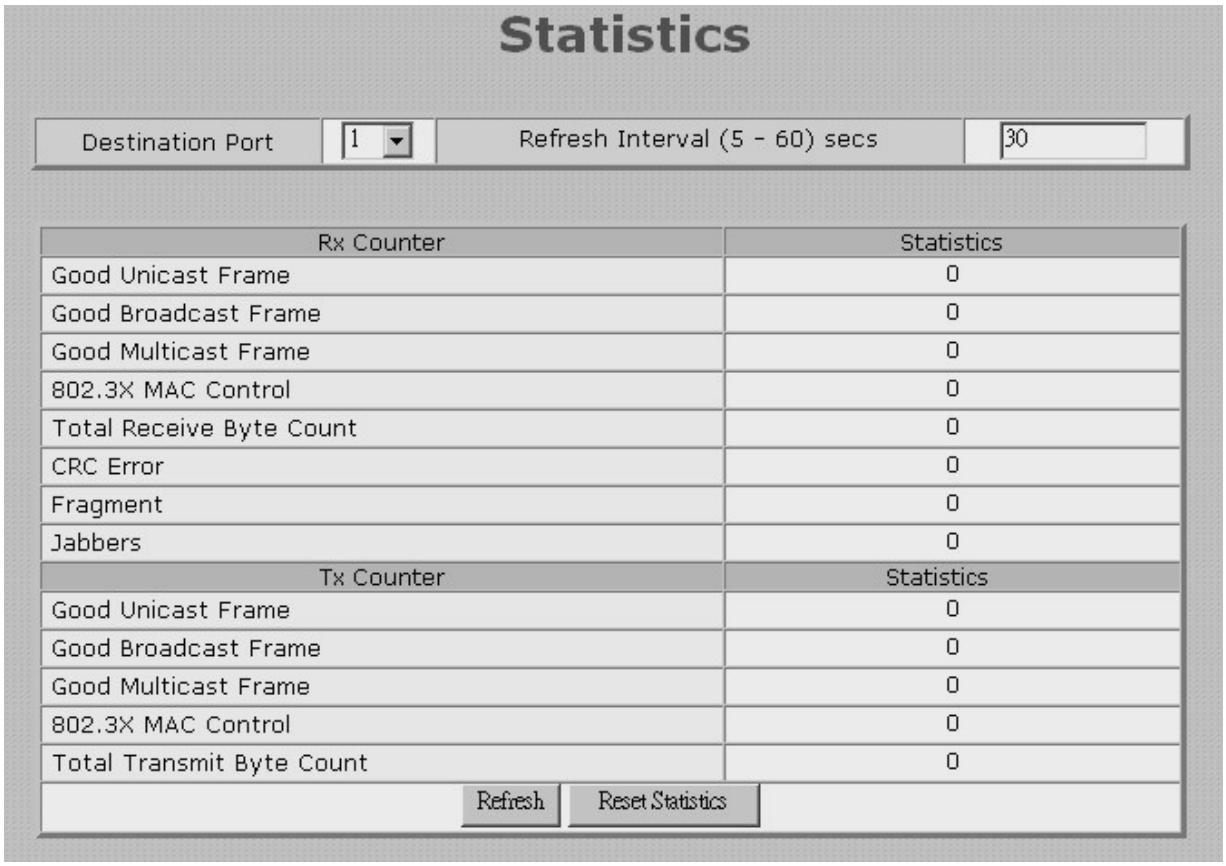
4. Supplicant Timeout Period:
   This is the timeout value between the switch and users (called “supplicant” in 802.1x) after first identification. The valid value is 0~65535.
5. Quiet Timeout Period:
   This is the quiet time value between the switch and the user before next authentication process when authentication fails.
6. Tx Timeout Period:
   This is the timeout value for the identification request from the switch to users. The request will be re-tried until the **Re-authentication Max Count** is met. After that, authentication fail message will be sent. The valid value is 0~65535.
7. Radius Server Configuration:
   This is the configuration for the switch to work with RADIUS server.



The Port Authentication Configuration is used to select the authentication mode for each port of the switch.

1. Auto: This is the normal 802.1x operation mode. The authentication status (authenticated or unauthenticated) depends on the authentication result of port.
2. Force-Authorized: This mode will force the port always being authentication successful in 802.1x process and the real authentication result will be ignored.
3. Force-Unauthorized: This mode will force the port always being authentication fail in 802.1x process and the real authentication result will be ignored.
4. None: This mode will disable 802.1x operation on this port.

16. Statistics

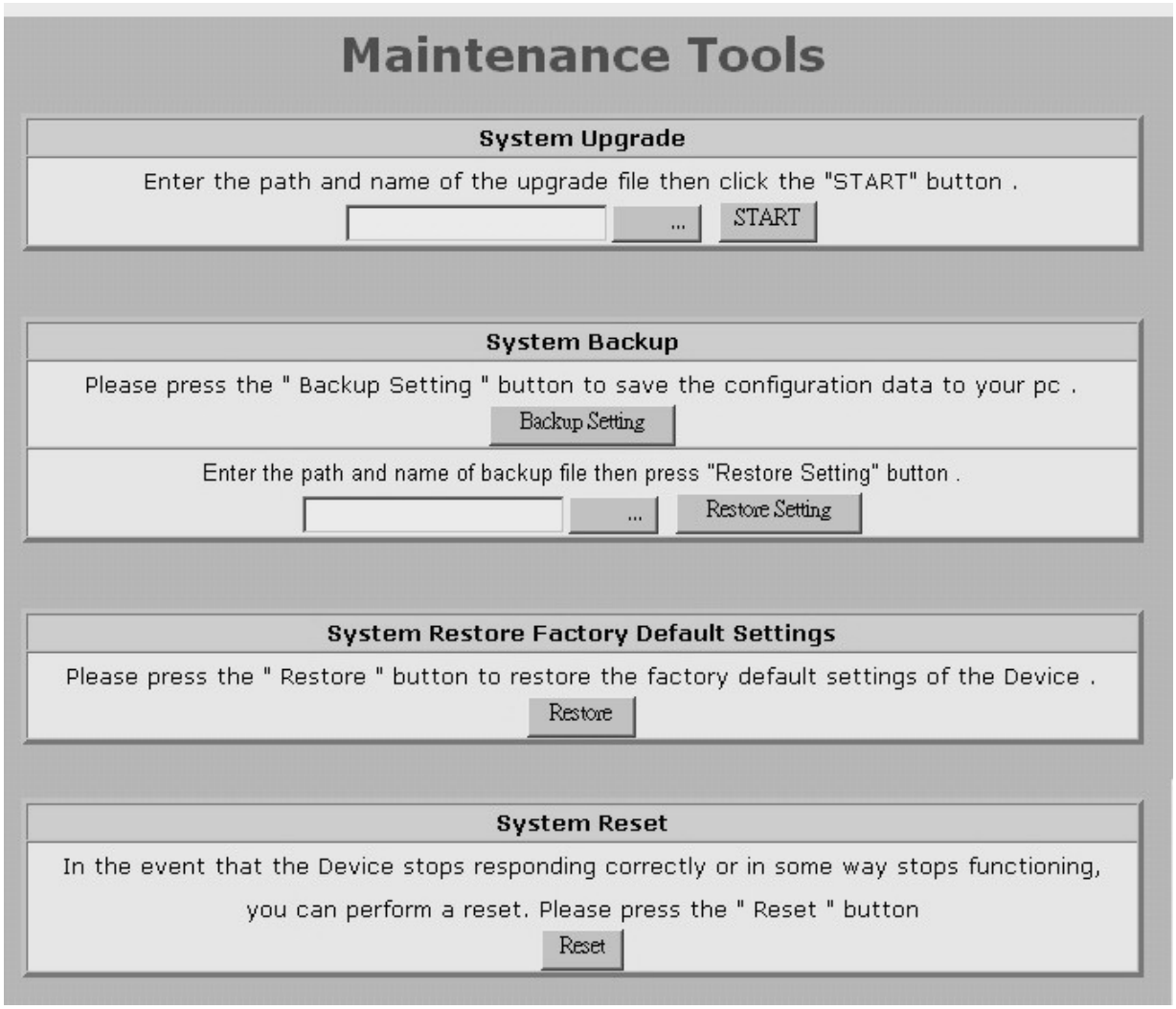


You can find the traffic statistics here. Select port number to get the counters for different port.

You can modify the refresh interval to get different counter updating period. Click “Refresh” button can update the counter immediately.

You can reset counters to zero with the “Reset Statistics” button.

17. Tools


Maintenance Tools
System Upgrade
Enter the path and name of the upgrade file then click the "START" button .
...
START
System Backup
Please press the " Backup Setting " button to save the configuration data to your pc .
Backup Setting
Enter the path and name of backup file then press "Restore Setting" button .
...
Restore Setting
System Restore Factory Default Settings
Please press the " Restore " button to restore the factory default settings of the Device .
Restore
System Reset
In the event that the Device stops responding correctly or in some way stops functioning,
you can perform a reset. Please press the " Reset " button
Reset

Four functions are supported as the system maintenance tools.

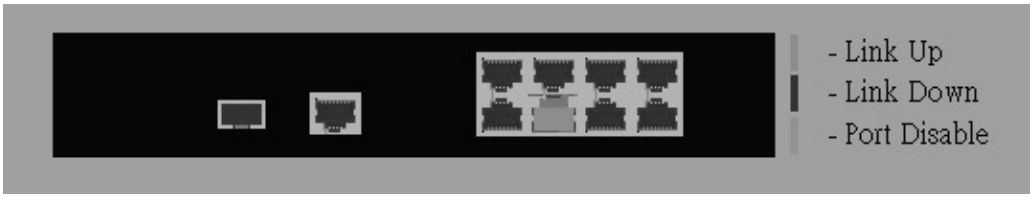
a. System Upgrade
This function will upgrade the system operation software from the web management PC.

b. System Backup
[Backup Setting] will backup the configuration of the switch to the web management PC.
[Restore Setting] will get the configuration backup file from the web management PC and restore it to the switch.

c. System Restore Factory Default Setting
This function will restore the switch configuration to factory default setting.

d. System Reset
This function will cause the switch reset.

18. Port Status Picture



At upper part of the web interface, there is a picture showing current status of each port – green for link-up, black for link-down and orange for disabled. With this picture, you can get current port status.

Click some of the port in the picture. The detail port configuration and status will be shown as following sample.

Port Summary

Port state summary

Port Number	Type	Link Status	Admin Status	Auto. Negotiation	Speed Status	Duplex Status	Flow Control
4	100TX	Up	Enable	Enable	100Mbps	Half	Disable

Port Statistics

In Octets	1535608	Out Octets	919564
In Unicast Pkts.	2652	Out Unicast Pkts.	1475
In Non-Unicast Pkts.	5958	Out Non-Unicast Pkts.	3
In Discards	0	Out Discards	0
In Errors	11	Out Errors	0
Alignment Errors	0	CRC Errors	0
Single Collisions	0	Multiples Collisions	0
Defered Transmissions	1	Late Collisions	0
Excess Collisions	0	Carrier Sense Errors	0
Drop Events	0	Fragments	11
Octets	1535608	Jabbers	0

Apply Refresh

6.4 About Telnet Interface

If you want to use Telnet to management the switch from remote site, you have to set the IP/Mask/Gateway address to the switch first from console. Then use "telnet <IP>" command in DOS. Its operation interface is the same as console interface.

6.5 About SNMP Interface

If you want to use NMS to management the switch from remote site, you have to set the IP/Mask/Gateway address to the switch and configure the SNMP setting of the switch from console first. Then you can use SNMP management program to manage this switch.

This switch supports SNMP Version 1 agent function and MIB II(Interface), Bridge MIB, Etherlike MIB and Private MIB. The default GET community name is “public” and SET community name is “private”.

This switch supports up to five trap receivers with different trap community names.

7. Software Update and Backup

This switch supports software/configuration backup and update/restore functions. It could be done in three ways.

1. From console when booting : by Xmodem protocol and doing by terminal program. This function can be used for run-time code and boot code updating. (Boot code works only at boot time - before the main program starts.)

   Press Ctrl-C when the switch is booting, the following message will be shown.

```
      Boot Menu
============================
0: Start the Run-time code
1: Upgrade Run-time code
2: Upgrade Boot Code

=> Select:
```

   a. *Start Run-time code* : This option will continue the booting process.

   b. *Upgrade Run-time code* : This option will try to update run-time code (main code) from terminal program with Xmodem protocol. If this option is selected, the following message will be shown.
   "Waiting to receive file by Xmodem ...."
   Then user can select Send File function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

   c. *Upgrade Boot Code* : This option will try to update boot code from terminal program with Xmodem protocol. User can select Send File function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

2. From console/Telnet when running : Doing by TFTP protocol and it will need a TFTP server in network. Please refer to the description of "*Upgrade*" function in console operation in Section 6.2.

3. From web browser : Doing by http protocol and by web browser. Please refer to the description of "*Tools*" function in Section 6.3.

A. Product Specifications

Access Method	Ethernet , CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000Base-T, IEEE 802.3z
MDI/MDIX	Auto-detect for each TX port
Indicator Panel	LEDs for each unit : Power each port : Link/Act, FDX
Number of Ports	8* RJ45 10/100M TX ports, 1* RJ45 10/100/1000M TX port, 1*1000M SFP(miniGBIC) port
Dimensions	250W x 117D x 37H mm
Certification	VCCI Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	5% to 95% (Non-condensing)
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	4K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	1536 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex
VLAN	Port-based, IEEE802.1Q
Multicast	IGMP Snooping
QoS	2 transmit queues per ports, for port-based/802.1P tagged-based priority operation
Spanning Tree	Support IEEE 802.1D protocol
Trunking	4 groups max.
Mirror Port	1 capture port for Ingress/Egress traffic, DA/SA filtering function is supported
SNMP	Ver. 1, Supports MIB II(Interface), Bridge MIB, Etherlike MIB, Private MIB
Security	IEEE802.1x Port security
Out-band Management	Console
In-band Management	Telnet, Http, SNMP
Software Update/Backup	by TFTP, Http protocol, Xmodem, for firmware / configuration

B. Compliances

EMI Certification

FCC Class A Certification (USA)

Warning: This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A digital device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are required to correct the interference.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014. It conforms to the following specifications:

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4kV CD, 8kV AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1kV - (power line), 0.5kV - (signal line)

This product complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC.

Warning! Do not plug a phone jack connector in the RJ-45 port. This may damage this device.

VCCI Warning

注意

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。